



# Cybersecurity in the Mekong region

An Analysis of the Legal Framework  
and Recommendations for the Protection  
of Indigenous Environmental  
Human Rights Defenders



INTERNATIONAL WORK GROUP  
FOR INDIGENOUS AFFAIRS



NICFI

Norway's International Climate and Forest Initiative





# **Cybersecurity in the Mekong region:** An Analysis of the Legal Framework and Recommendations for the Protection of Indigenous Environmental Human Rights Defenders

*May 2021*



**INTERNATIONAL WORK GROUP  
FOR INDIGENOUS AFFAIRS**



# **Cybersecurity in the Mekong region:** An Analysis of the Legal Framework and Recommendations for the Protection of Indigenous Environmental Human Rights Defenders

Copyright © Asia Indigenous Peoples Pact 2021

The contents of this publication may be reproduced and distributed for non-commercial purposes with the prior notice to the copyright holder and the source and authors are duly acknowledged

## **Published by:**

Asia Indigenous Peoples Pact (AIPP)  
112 Moo 1, Tambon Sanpranate, Amphur Sansai,  
Chiang Mai 50210,  
Thailand  
Tel: +66 (0) 53 343 539  
Fax +66 (0) 53 343 540  
[www.aippnet.org](http://www.aippnet.org)

**Edited by:** Prabindra Shakya

## **Written by:**

Emilie Pradichit, Manushya Foundation – Cambodia, Lao PDR, Thailand and Vietnam country chapters  
and Open Development Initiative – Myanmar country chapter

## **Photo credits:**

Thailand : Phnom Thano and Indigenous Media Network (IMN)  
Vietnam : <https://unsplash.com/s/photos/vietnam>  
Myanmar : AIPP and <https://unsplash.com/s/photos/myanmar>  
Cambodia : Cambodia Indigenous Peoples Alliance (CIPA) and Bunong News Network (BNN)  
Laos : <https://unsplash.com/s/photos/laos>

## **Supported by:**

Norway's International Climate and Forest Initiative (NICFI)

**Disclaimer:** The contents of this publication are the sole responsibility of the Asia Indigenous Peoples Pact (AIPP) and cannot be taken to reflect the views of the donors. The sharing of this publication with the external audience is aimed at sharing general information and recommendations and does not constitute an endorsement by the donors or its institutions.

**Layout and Printing:** AIPP Printing Press Co., Ltd Chiang Mai, Thailand

# Contents

Acknowledgement .....	4
Acronyms .....	5
I. Introduction .....	7
II. Status of identification of Indigenous Peoples in the Mekong region and recognition of their rights.....	8
III. Overview of the situation of IEHRDs .....	13
IV. IEHRDs and Cybersecurity laws and policies .....	18
V. Recommendations.....	30
<b>CAMBODIA.....</b>	<b>35</b>
1. Introduction .....	36
2. Methodology .....	40
3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age.....	41
4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases .....	48
5. Recommendations .....	52
<b>Lao PDR.....</b>	<b>55</b>
1. Introduction .....	56
2. Methodology .....	60
3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age.....	61
4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases .....	68
5. Recommendations .....	72
<b>MYANMAR .....</b>	<b>77</b>
1. Status of legal recognition of the rights and identities of Indigenous Peoples .....	78
2. Overview of the situation of IEHRDs.....	81
3. Methodology used for the formulation of the study.....	85
4. Indigenous Environment Human Rights Defenders (IEHRDs) and Cybersecurity law and policies.....	86
5. Recommendations .....	97
<b>THAILAND.....</b>	<b>103</b>
1. Introduction .....	104
2. Methodology .....	108
3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age.....	109
4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases .....	117
5. Recommendations .....	122
<b>VIETNAM .....</b>	<b>125</b>
1. Introduction .....	126
2. Methodology .....	129
3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age.....	130
4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases .....	135
5. Recommendations .....	138
<b>References.....</b>	<b>141</b>

# Acknowledgement

Asia Indigenous Peoples Pact (AIPP) is very grateful to all individuals – Indigenous brothers and sisters, member and, partner organizations and funding agencies for providing necessary technical and financial support in research, documentation and also making possible to publish this book 'Cybersecurity in the Mekong region: An Analysis of the Legal Frameworks and Recommendations for the Protection of Indigenous Environmental Human Rights Defenders a reality'.

In particular, AIPP would like to thank the Authors, Ms. Emilie Pradichit of Manushya Foundation. From the Open Development Initiative (ODI) team Mr. Saw Ar Htite, Myanmar chapter and Ms. Mia Chung and Ms. Pyrou Chung for their collective research and editorial contributions. The editor Mr. Prabindra Shakya for the invaluable support in the process of research, documentation and finalization of the book in the publishable form, without their continuous and tireless efforts it wouldn't be possible. We acknowledge and appreciate the solidarity and cooperation of the members and partners, especially, from Cambodia, Lao PDR, Myanmar, Thailand and Vietnam for the providing photos and valuable inputs. Last but not the least, we would like to thank the AIPP management and Environment program for all necessary cooperation and guidance provided throughout the study and publication of this book.

The production of this book would not have been possible without the generous financial support and cooperation of International Work Group for Indigenous Affairs (IWGIA) and Norway's International Climate and Forest Initiative (NICFI). We wish continuous support and cooperation of IWGIA and NICFI in future as well.

# Acronyms

<b>AIPP</b>	Asia Indigenous Peoples Pact	<b>Lao PDR or Laos</b>	Lao People's Democratic Republic
<b>CCA</b>	Computer Crime Act	<b>LOCS</b>	Law On Cybersecurity
<b>CEDAW</b>	Convention on the Elimination of All Forms of Discrimination against Women	<b>MEDS</b>	Ministry of Digital Economy and Society
<b>CLT</b>	Community Land Titling	<b>mmCERT</b>	Myanmar Computer Emergency Response Team
<b>CMO</b>	Committee Managing the Office of the National Cybersecurity Committee	<b>MOU</b>	Memorandum of Understanding
<b>CPP</b>	Cambodian People's Party	<b>MoTC</b>	Ministry of Transportation and Communication
<b>CRC</b>	Cybersecurity Regulation Committee	<b>MPTC</b>	Ministry of Post and Telecommunications of Cambodia
<b>CSO</b>	Civil Society Organization	<b>NBTC</b>	National Broadcasting and Telecommunications Commission
<b>CSL</b>	Cyber Security Law	<b>NCPO</b>	National Council for Peace and Order
<b>EHRD</b>	Environmental Human Rights Defender	<b>NCSC</b>	National Cyber Security Committee/Center
<b>EIA</b>	Environmental Impact Assessment	<b>NGO</b>	Non-Governmental Organization
<b>ELC</b>	Economic Land Concession	<b>NHRCT</b>	National Human Rights Commission of Thailand
<b>FPIC</b>	Free, Prior and Informed Consent	<b>NIG</b>	National Internet Gateway
<b>HRC</b>	Human Rights Committee	<b>NLA</b>	National Legislative Assembly
<b>HRD</b>	Human Rights Defender	<b>OHCHR</b>	Office of the High Commissioner on Human Rights
<b>GBV</b>	Gender-Based Violence	<b>PDPA</b>	Personal Data Protection Act
<b>ICCPR</b>	International Covenant on Civil and Political Rights	<b>SAC</b>	State Administration Council
<b>ICESCR</b>	International Covenant on Economic, Social and Cultural Rights	<b>SDG</b>	Sustainable Development Goal
<b>ICT</b>	Information and Communications Technology	<b>SLAPP</b>	Strategic Lawsuit Against Public Participation
<b>IEHRDs</b>	Indigenous Environmental Human Rights Defenders	<b>UDHR</b>	Universal Declaration of Human Rights
<b>ILO</b>	International Labour Organization	<b>UN</b>	United Nations
<b>IO</b>	Information Operation	<b>UNDRIP</b>	UN Declaration on the Rights of Indigenous Peoples
<b>IPs</b>	Indigenous Peoples	<b>UNGPs</b>	UN Guiding Principles on Business and Human Rights
<b>ISP</b>	Internet Service Provider	<b>VFV</b>	Virgin Fallow and Vacant
<b>ITCSD</b>	Information Technology and Cyber Security Department	<b>VPN</b>	Virtual Private Network
<b>IWGIA</b>	International Work Group for Indigenous Affairs		
<b>KKNP</b>	Kaeng Krachan National Park		
<b>KNU</b>	Karen National Union		
<b>LANGO</b>	Law on Associations and Non-Governmental Organizations		







# I. Introduction

This report is part of “Defending the Defenders: Indigenous Environment Human Rights Defenders (IEHRDs)” project of the Asia Indigenous Peoples Pact (AIPP) and the International Work Group for Indigenous Affairs (IWGIA). It aims to review the existing legal frameworks regulating cyber security and its application in the Mekong countries with special focus on IEHRDs; to identify specific risks, legal frameworks regulating cyber security in these countries may pose to IEHRDs, and to develop practical recommendations for the IEHRDs to mitigate cybersecurity risks, while ensuring and exercising their right to freedom of expression. While the principal objective of the publication is to raise awareness and build capacity of Indigenous Peoples, it could also be useful for advocacy work at different levels.

While the particular focus of the report is on human and environmental rights defenders belonging to Indigenous groups, it also covers non-indigenous environmental rights defenders in the Mekong countries – Cambodia, Myanmar, Lao PDR, Thailand and Vietnam.

The methodology used for this report includes desk research for all the country chapters, including a systematic literature review of relevant laws and government regulations, reports and observations/recommendations of United Nations (UN) human rights bodies and NGOs, news reports, expert papers and other publications. Primary data, including testimonies and cases of IEHRDs facing challenges to their cybersecurity, were collected from the activities organized by the AIPP and the Manushya Foundation. For example, AIPP organized a regional exchange and training on digital security from 30 September to 2 October 2020, where IEHRDs from ten countries participated and shared their experiences with online interferences, including threats, prosecution, hacking and internet shutdown, in relation to their work on Indigenous rights. Interviews and consultations with IEHRDs were undertaken at local and national levels for the country chapters on Cambodia, Lao PDR, Thailand and Vietnam that the Manushya Foundation prepared.

However, for the Myanmar chapter prepared by the Open Development Initiative, key informant interviews with Indigenous Peoples’ representatives could not be undertaken due to the current unsafe political situation in the country following the February 2021 coup. An external consultant was commissioned to review the country chapters, make additional analysis as needed and consolidate the regional analysis into a final report.

## II. Status of identification of Indigenous Peoples in the Mekong region and recognition of their rights

In the Mekong region, while Cambodia provides some recognition for Indigenous Peoples in its legal and policy framework, rest of the countries do not officially recognize Indigenous Peoples as such. In national laws and policies, they are often referred to as “national races” or “ethnic groups” in Myanmar, “ethnic groups” in Lao PDR, “hill tribes”, “ethnic groups/communities” in Thailand and “ethnic minorities” in Vietnam.

In terms of numbers, as per government data, those who identify as Indigenous Peoples in the Mekong countries range from as little as around at least 1.4 percent of the total population in Cambodia to as high as between 35 and 70 percent of Lao PDR’s population. However, in lack of legal recognition and reliable official statistics, the number of Indigenous groups and their shares in the national population are contested while a number of groups are increasingly identifying themselves as Indigenous Peoples and their movements are emerging. For example, there are 56 ethnic groups across Thailand that continue to use traditional practices and pass on their folk wisdom from generation to generation and account for 6.1 million people or 9.68 percent of the total national population. The indigenous movement in Thailand that started with ten “hill tribes” has now grown to 40 Indigenous groups and thus has the potential to represent all the 56 ethnic groups.<sup>1</sup>

**Table 1:** Number of Indigenous groups and their population in Mekong region.

Country	Common external designation	Number of ethnic groups	Estimated total population and share of national population
Cambodia	Indigenous minorities	24	170,000 (1.4%)
Myanmar	Ethnic nationalities or minorities	135	Between 14.4 and 19.2 million (30 – 40%)
Lao PDR	Ethnic minorities	Around 200 (49 officially recognized “ethnic minorities”)	Between 2.3 and 4.6 million (35-70%)
Thailand	Ethnic Minorities, Hill Tribes, Hill/ Mountain People	Over 25 (10 officially recognized “hill tribes”)	Around 5 million (7.2%)
Vietnam	Ethnic minorities	Over 90 (53 officially recognized “ethnic minorities”)	12.3 million (13.23%)

Adapted from AIPP and IWGIA<sup>2</sup>

1 Micah F. Morton, *The Indigenous People’s Movement in Thailand Expands*, ISEAS, 16 December 2016, available at: [https://www.iseas.edu.sg/images/pdf/ISEAS\\_Perspective\\_2016\\_68.pdf](https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2016_68.pdf)

2 Some figures revised as per IWGIA, *The Indigenous World*, 2020

None of the Mekong countries contain any specific reference to Indigenous Peoples or their rights in their Constitutions. Recently, there has been little progress in some of these countries in terms of legal and policy reforms relevant to Indigenous Peoples. However, they still fail to meet the international human rights standards. At the same time, there are longstanding laws and policies, which contravene or limit the rights of Indigenous Peoples, including to their lands and resources. New laws and policies have also been adopted that negatively impact indigenous rights. Besides limited legal protections of their rights, Indigenous Peoples in the region continue to face human rights challenges due to extra-legal and corrupt practices of their governments.

## Cambodia

The 1993 Cambodian Constitution includes some provisions relevant for Indigenous Peoples, including guarantee of collective ownership of immovable property and recognition of the right to fair and prior compensation to both individual and collective owners (Article 44). The 2001 Land Law guarantees the recognition and protection of Indigenous communities (“original ethnic minority”), traditional natural resource management systems and traditional customary land, as well as provides for collective land titling for communal lands of indigenous communities. As of March 2021, a total of 27 communities held legally recognized communal land titles, which is only a fragment of communal land of more than 500 indigenous communities without such titles.<sup>3</sup>

The Forestry Law of 2002 contains provisions for official recognition of community forestry and offers communities an opportunity to obtain user and management rights to forests. It also includes special provisions on “nomadic agriculture” within collectively owned land. In 2009, Cambodia has adopted a National Policy on the Development of Indigenous Peoples to ensure that the rights of Indigenous Peoples are safeguarded, and their livelihoods and quality of life promoted across all sectors. However, Indigenous Peoples continue to face challenges to their rights, including and particularly due to large number of economic land concessions that the government grants to agribusiness, mining and other companies. Such concessions granted without Free, Prior and Informed Consent (FPIC) of the concerned communities have resulted in forced evictions, loss of lands and livelihoods for the communities. Recent political developments, which has practically placed the country under a one-party rule, has worsened the situation for Indigenous Peoples and their rights defenders.

## Myanmar

Myanmar’s 2008 Constitution states that the Union shall assist to develop language, literature, fine arts and culture of the national races, as well as to promote socio-economic development of less-developed national races (Article 22). Kachin, Kayin/Karen, Shan, Mon, Kayah/Karenni, Chin, Burman and Arakan are considered as national races, which are broken down into 135 ethnic groups.<sup>4</sup> The 1982 Burma Citizenship Law states that the nationals of those races and ethnic groups that have settled in any of the territories within the State prior to 1823 are Burma citizens. The 2015 Protection of the Rights of National Races Law includes

---

3 Open development Cambodia, Registered indigenous communal land, available at: <https://data.opendatacambodia.net/en/dataset/registered-indigenous-communal-land/resource/ad186575-e436-4a12-a01c-90353261719d>

4 See the breakdown table of the national races in the Myanmar country chapter below.

as one of its purposes “to aim for the socio-economic development of less-developed national races”. It uses the term “Indigenous Peoples” (hta-nay tain-yin-tha), which does not appear in other laws, but is undefined. It discusses providing equal rights to all national races but does not include any protection from discrimination. Reportedly developed without consultation with Indigenous Peoples<sup>5</sup>, the law lacks clarity.

The 2016 National Land Use Policy is considered a landmark policy, which includes a chapter on “Land Use Rights of Ethnic Nationalities” referring to the customary land tenure rights of ethnic nationalities and land-use mapping. It also mentions Free, Prior, Informed and Consent (FPIC) as a means of addressing “land monopolization and speculation”, and establishes a process for recognition of the rights of Indigenous communities and not just individuals. On the other hand, the 2012 Virgin Fallow and Vacant Land Law allows the government to take possession of unregistered land across the country. Approximately 75% of virgin, fallow and vacant land are in the seven ethnic states, which are highly impacted by the law.<sup>6</sup> Amendments to the law in 2019 require registration processes that remote-dwelling Indigenous communities are unaware of and are unable to meet due to inadequate support for documentation.

Indigenous Peoples in Myanmar have been fighting for their rights, including to self-determination, since Myanmar’s independence. The post-1962 military junta’s implementation of “Burmanization” and ethnic armed conflicts have caused a wide range of human rights violation of Indigenous Peoples, including extrajudicial killings, mass displacement, etc. However, even after democratic opening in 2015, Indigenous communities continued facing challenges to their rights, including to their land and resource rights, with earlier or newly approved extractive and other projects in their territories. Following the recent military coup in February 2021, prospects for overall human rights situation in the country appear dim.

## Lao PDR

As per the Lao PDR’s 2015 Constitution, all ethnic groups have the right to protect, preserve and promote the fine customs and cultures of their own tribes and of the nation, and acts creating division and discrimination among ethnic groups are prohibited. The State pursues the policy of promoting unity and equality among all ethnic groups and implements every measure to gradually develop and upgrade the socio-economic levels of all ethnic groups (Article 8). The 2003 Land Law states that land of the Lao PDR is under the ownership of Lao population, in which the State is charged with centralized and uniform management and allocation of land for use, lease or concession.<sup>7</sup> While the law recognizes permanent and temporary land-use rights for individuals, it fails to define communally held rights of Indigenous communities.<sup>8</sup> The 2018 Law on Resettlement and Vocation allows for “general resettlement” of communities residing in “remote and underdeveloped areas”, which

---

5 Donna Guest, *Briefing Paper: Indigenous Peoples’ Rights and Business in Myanmar*, 2016, available at: [https://themimu.info/sites/themimu.info/files/documents/Paper\\_Indigenous\\_Peoples\\_Rights\\_Business\\_in\\_Myanmar\\_Feb2016\\_ENG.pdf](https://themimu.info/sites/themimu.info/files/documents/Paper_Indigenous_Peoples_Rights_Business_in_Myanmar_Feb2016_ENG.pdf)

6 International Work Group for Indigenous Affairs, *Indigenous Peoples and land rights in Myanmar*, 2020, available at: <https://www.iwgia.org/en/myanmar/3904-indigenous-peoples-and-land-rights-in-myanmar.html>

7 Manushya Foundation and AIPP, *Lao UPR Factsheet on Indigenous Peoples’ Rights*, January 2020, available at: <https://www.manushyafoundation.org/lao-pdr-upr-factsheets>

8 IWGIA, *Indigenous World 2020: Laos*, 11 May 2020, available at: <https://www.iwgia.org/en/laos/3604-iw-2020-laos.html>

expands the government's authority to relocate communities, especially ethnic groups, to suit development projects and business investments.<sup>9</sup>

The Government in March 2020 adopted a Decree on Ethnic Groups, which includes provisions to enforce comprehensive support to ethnic groups in rural areas, such as access to infrastructure, education, health, information, justice and gender. However, the Decree neither addresses the rights of Indigenous Peoples to their lands, resources and traditional livelihoods nor ensures education in different ethnic languages. Some provisions could even worsen the situation of Indigenous ethnic groups as the Decree advises "to resettle ethnic groups that live in the hardship and undeveloped areas, risky livelihoods areas, development project-affected areas, and special areas to areas that can be developed and create appropriate permanent jobs and employment".<sup>10</sup>

## Thailand

The 2017 Constitution of Thailand states that the State should promote and provide protection for different ethnic groups to have the right "to live voluntarily and peacefully without disturbances in the society according to their culture, custom and traditional ways of life, insofar as it is not contrary to public order or good morals of people, or does not harm the security of the State, health or sanitation" (Section 70). The Constitution did away with the reference to "traditional communities" in the earlier Constitution but has continued provisions for rights of communities, including to conserve, revive or promote their culture, tradition and good customs; as well as to manage, maintain and utilize natural resources, environment and biodiversity in a balanced and sustainable manner (Section 43).

Despite recent positive legal and policy reforms in relation to the Nationality Act, many people belonging to Indigenous groups still face challenges to obtain citizenship and remain stateless, which continues as a major problem. Those without citizenship or other legal status are also denied access to basic services and fundamental rights and freedoms. Further, laws, including Land Code (1954), Forest Act (1941), National Park Act (1961), National Reserved Forest Act (1964), Wild Animal Preservation and Protection Act (1992), limit the rights of Indigenous communities to their lands and resources, particularly to forests in protected areas. The 2014 military junta orders related to ending deforestation and encroachment on forest reserves have also resulted in large number of forced evictions. At the same time, the 2019 amendments to the National Park and Wildlife Preservation and Protection Acts have also been contentious with the forest dependent communities and their groups.<sup>11</sup> Although the recently adopted Community Forest Act can be considered somewhat positive to provide for community forest management, the law is inadequate and does not meet international standards of Indigenous rights.<sup>12</sup>

Earlier, in 2010, the government adopted the Regulation of the Prime Minister's Office on the issuance of Community Land Title Deeds to provide for communities' management of State-owned lands for their livelihoods with land-use permits. However, as of 2012, more than 400 local communities were in waiting for community land title deeds, and only 55

---

9 See Lao PDR country chapter below

10 IWGIA, *Indigenous World 2020: Laos*, 11 May 2020, available at: <https://www.iwgia.org/en/laos/3604-iw-2020-laos.html>

11 Indigenous Women's Network of Thailand (IWNT) and Manushya Foundation, *Raising Our Voices to Save Our Future*, September 2019, available at: <https://www.manushyafoundation.org/iwnt-report>

12 Prabindra Shakya, *Study on the National Legal and Policy Framework on the Rights of Indigenous Peoples in Thailand*, AIPP, (forthcoming)

community land titles were approved.<sup>13</sup> Similarly, the 2010 Cabinet Resolutions on the Restoration of Traditional Practices and Livelihoods of Chao Lay and Karen in Thailand include measures related to ethnic identities and cultures, natural resources management, right to nationality, cultural heritage preservation, and education for those groups. However, the implementation of these resolutions has so far been slow and ineffective because of, among others, bureaucratic obstacles and political instability, lack of awareness of concerned government agencies, the need for coordination across different ministries and the low budget allocated for the activities.<sup>14</sup>

## Vietnam

Vietnam's 2013 Constitution refers to Indigenous Peoples as "ethnic minorities". It recognizes the right of every ethnic group to use their own language and writing, to preserve their ethnic identity and to nurture their fine customs, traditions and culture, and the State obligation to provide the conditions for the development of ethnic minorities. The Government has adopted a number of specific programs targeting ethnic minorities in order to bridge existing social and economic gaps between them and the rest of the population. It has also established two dedicated bodies to deal with ethnic minority issues, namely the National Assembly's Council on Ethnic Minorities and the ministerial Committee for Ethnic Minority Affairs. The policies adopted have, however, been seen to be aimed at integrating ethnic minorities into mainstream society rather than enabling them to strengthen their own institutions.<sup>15</sup>

Despite government programs targeting ethnic minorities over the years, they are still significantly poorer than the majority population. On the other hand, human rights organizations report frequent harassment of Indigenous communities by the State authorities for speaking about their rights or merely criticizing the government's actions or the Party. Some Indigenous communities, such as the Montagnards, are also persecuted due to their history, ethnicity or their religious beliefs.<sup>16</sup>

---

13 Ibid

14 IWGIA, *Indigenous World 2016: Thailand*, 2016, available at: [https://www.iwgia.org/images/publications/0740\\_THE\\_INDIGENOUS\\_WORLD\\_2016\\_final\\_eb.pdf](https://www.iwgia.org/images/publications/0740_THE_INDIGENOUS_WORLD_2016_final_eb.pdf)

15 Stefania Errico, *The rights of indigenous peoples in Asia: a human rights-based overview of national legal and policy frameworks against the backdrop of country strategies for development and poverty reduction*, ILO, 2017, available at: [https://www.ilo.org/global/publications/WCMS\\_545487/lang-en/index.htm](https://www.ilo.org/global/publications/WCMS_545487/lang-en/index.htm)

16 See the Vietnam country report below for more information

### III. Overview of the situation of IEHRDs

IEHRDs in Mekong countries comprise of members of Indigenous and other communities, Indigenous activists and leaders, environmental activists, representatives of NGO/CSOs, journalists, women's rights activists as well as democracy and peace activists, among others. They raise their own voices or support advocacy of the concerned communities against land grabbing, forced evictions, deforestation and environmental destruction, and abuse of human rights, including women's rights, in the name of development or conservation projects and business investments, as well as for protection of the nature, democratization and peacebuilding in general.

Despite differences in national political contexts in the Mekong region, the IEHRDs face similar challenges due to increasingly shrinking civic space and threats and reprisals as a result of their work. Civic space has further shrunk in recent years, including due to recent political changes such as the February 2021 military coup in Myanmar and quashing of political opposition in Cambodia since 2017, as well as in the name of the COVID-19 pandemic response more recently. Most Mekong countries have a longstanding record of targeting critics, including political opposition and activists, human rights defenders, journalists and others. That has even resulted in an environment of widespread fear, whereby dissent is rare such as in the context of Lao PDR. Specifically, after the disappearance of the prominent civil society leader Sombath Somphone in December 2012, Lao activists and civil society generally exercise self-censorship for the fear of reprisals.<sup>17</sup> At the same time, the Lao government owns most of the media outlets in the country and private media undergo strict censorship and may face penalties for dissident political commentary while there is lack of independent and effective judicial system for remedies.<sup>18</sup>

IEHRDs and the communities they work with have often become particular targets of the governments as they mostly challenge the laws, policies and practices related to lands and resources, which contrasts with the State aspiration to control them as well as business interests over them. In lack of legal recognition of or respect for the rights of Indigenous communities as well as strong push for economic growth in the Mekong countries, the communities and their supporting IEHRDs are caught up in land and resource conflicts with the State and business entities. During the course of the legitimate resistance to defend human and environmental rights, IEHRDs encounter a series of challenges for their works as well as face risks and reprisals. Those challenges and reprisals often begin with social stigmatization against the IEHRDs as "anti-development" and "anti-national" and include harassment, threats, attacks, arbitrary arrests and detentions, prosecution and even enforced disappearances and killings of the IEHRDs.

With the advancement of information technologies in the region and specifically in the context of the ongoing global COVID-19 pandemic, IEHRDs and their communities in Mekong countries have increasingly turned to digital and online spaces for their daily and activism work. Social media and instant messaging apps have become prominent tools for

---

17 Human Rights Council, Working Group on Arbitrary Detention, *Opinion No. 61/2017 concerning Lodkham Thammarong, Somphone Phimmasone and Soukan Chaitad (Lao People's Democratic Republic)*, 15 September 2017, available at: [https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A\\_HRC\\_WGAD\\_2017\\_61.pdf](https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_61.pdf)

18 See Lao PDR country chapter below for more information



advocacy and mobilization. Digital technologies have opened new avenues for recording and reporting abuses of rights. For example, the Prey Lang Community Network in Cambodia, a loosely structured network of Indigenous Kouy and Khmer villagers, has used a specially designed app with a security component to document illegal logging since 2015. The app allows IEHRDs and villagers to report and record threats, intimidation and violence related to their forest protection activities, combined with relevant data drawn to assess the situation faced by members.<sup>19</sup>

On the other hand, the governments of the Mekong countries have also been expanding their control over the cyberspace to stifle online freedom of expression and privacy. They have begun cracking down on online activism critical of the government and its activities through use of existing laws and policies as well as adoption of new ones, specifically on cybersecurity. While the countries already had legal restrictions on the enjoyment of fundamental rights to freedom of expression, association and peaceful assembly, they have adopted new laws and policies that further empower governments and their agencies to limit access to information through blocking or censorship of online content, monitor online communications and criminalize online speech on various grounds.

In Cambodia, for example, before the 2018 national elections, 17 news websites were blocked for 48 hours due to alleged “provocative” and “very political” news coverage.<sup>20</sup> Amid the COVID-19 pandemic, the government blocked Monoroom.info, a France-based Khmer-language news in March 2020 for reporting on the COVID-19 situation.<sup>21</sup> It also revoked licenses of several news outlets due to their reporting on issues such as land disputes and COVID-19 that was critical of the government while there are also reports of individuals made to take down critical online content after pressure from the police.<sup>22</sup>

Likewise, Vietnam’s Department of Information and Communications investigated more than 650 people and fined more than 160 people for sharing alleged “misinformation” in relation to COVID-19, which they were also forced to delete. Additionally, 47 bloggers, human rights defenders and journalists were arrested for their online activities and placed in pre-trial detention. The number of prisoners of conscience in the country also reached the highest in 2020 to 170 – among them, at least 69 were imprisoned due to online activism and 30 were women.<sup>23</sup>

In above contexts, the IEHRDs and their communities in the Mekong countries are currently facing risks and challenges, which are also extended in the cyberspace. Some representative IEHRDs in the region, who are experiencing reprisals for their works in the online and offline spaces, include<sup>24</sup>:

---

19 Prey Lang Community Network (PLCN), *The status of Prey Lang. 7th Monitoring*, 2019, available at: <https://preylang.net/wp-content/uploads/2019/01/7th-Monitoring-Report.pdf>

20 Committee to Protect Journalists, *CPJ condemns pre-election news censorship in Cambodia*, 30 July 2018, available at: <https://cpj.org/2018/07/cpj-condemns-pre-election-news-censorship-in-cambo/>

21 Reporters without Borders, *Cambodia: Hun Sen uses Covid-19 crisis to tighten his grip*, 9 April 2020, available at: <https://rsf.org/en/news/cambodia-hun-sen-uses-covid-19-crisis-tighten-his-grip>

22 Freedom House, *Freedom on the Net: Cambodia*, 2020, available at: [https://freedomhouse.org/country/cambodia/freedom-net/2020#footnoteref3\\_890of4y](https://freedomhouse.org/country/cambodia/freedom-net/2020#footnoteref3_890of4y); Phnom Penh Post, *Rapper Deletes Song Critical of Cambodian Social Issues*, 20 May 2019, available at: <https://www.phnompenhpost.com/national/rapper-deletes-song-critical-cambodian-social-issues>

23 See Vietnam country chapter below.

24 More information on most of the IEHRDs and the challenges they are facing in relation to cybersecurity are described in the respective country chapters.

- Ethnic Bunong activist Kroeung Tola of Cambodia, who is currently facing criminal charges of defamation for online criticism of the local district governor for clearing protected forests – he is planning to appeal against the charges;
- Three environmental defenders with the Mother Nature Cambodia, who await trial in detention, after their bail requests were denied by the court, on charge of “incitement to commit a felony or cause social unrest” based on a Facebook post regarding plan for a one-person march to the Prime Minister’s residence to call for an end to the exploitation of the Boeung Tamok Lake;
- Karen woman human rights defender Naw Ohn Hla in Myanmar, who has been jailed more than at least eight times since 1989 for her activism, including in pro-democracy protests, against killing of a local woman during demonstration against Chinese copper mining and recently for commemoration of Karen Martyrs’ Day in 2019;
- Environmental and woman human rights defender Houayheuag Xayabouly “Muay” of Lao PDR, who is presently serving her five-year prison sentence for the offence of “conducting propaganda activities against Lao PDR” due to her online criticisms of the government authorities, including in relation to their mishandling of the 2018 dam collapse at the Xe-Pian Xe-Namnoy hydropower project;
- Karen environmental and community activist Porlajee “Billy” Rakchongcharoen of Thailand, who was disappeared in 2014 in relation to his advocacy against destruction of houses and forced evictions of Karen communities living in Kaeng Krachan National Park, and recently proven as murdered five years later;
- Four students of Thailand’s Maejo University, who are facing defamation charges from the mining company 99 Tuwanon Co. Ltd. after they published their studies on impact of coal mining on Karen communities in Chiang Mai’s Omkoi district on Prachatai online website exposing how the locals were manipulated to sell their land to the company without knowledge and later threatened to stay silent;
- Environmental human rights defender Nguyen Ngoc Anh of Vietnam, who received six-year jail term in 2019 for reporting on Taiwanese company Formosa Plastics Group’s toxic waste spill into open ocean; as well as Dinh Thi Thy Thuy, who remains in pre-trial detention for sharing her opinions on Facebook on the Formosa environmental disaster, environmental issues in her hometown, government’s handling of the COVID-19 pandemic, etc.

Women IEHRDs and Indigenous women face greater vulnerability to the risks and reprisals due to their activism to defend their rights, including in the online sphere. Deeply embedded gender biases rooted in patriarchal beliefs and practices in Mekong countries impact the way women are able to engage publicly.<sup>25</sup> That also particularly affect their access to digital tools, including for women IEHRDs, whereby men in their lives often act as the gatekeepers of those tools. Studies show that barriers to owning and using a mobile phone to access the internet include affordability, literacy skills, and security and safety while gender norms perpetuate the inequality against women in the cyberspace.<sup>26</sup> Indigenous

25 Mia Chung and Pyroun Chung, *Mekong women in open data*, 2020, available at: <https://data.opendevlopmentmekong.net/dataset/mekong-women-in-open-data/resource/74805dc6-d1e8-44a3-8290-e31d5da5f070>

26 GSM Association, *The Mobile Gender Gap Report 2019*, February 20, 2019, available at: <https://www.gsma.com/>

women, particularly in the remote areas, will have even little access to such tools and online platforms. At the same time, women IEHRDs are more likely to suffer gender-based violence such as sexual harassment, assault and rape. That also extends to the cyberspace, whereby they are subjected to online harassment and abuse in lack of effective legal protections and knowledge of digital security measures. In Myanmar, women human rights defenders have reported of regular gender-based intimidation and threats of violence online, including cyberstalking, phishing, hacking and attempts for character assassination.<sup>27</sup>

Furthermore, besides blocking or censorship of content, monitoring of communications and criminalization of speech in online platforms with the use of various laws and policies, there are also reports of State-sponsored disinformation and hate speech in cyberspace targeting government critics, human rights defenders and journalists in Mekong countries. For example, in Thailand, the Army's Internal Security Operations Command has been carrying out Information Operations (IOs) to conduct cyber warfare against activists, politicians and academics by funding military-linked accounts publishing posts, stories and articles critical of them, as well as manipulating information and disseminating hate speech. The IOs aim to defame, disqualify and destroy the legitimacy and reputation of the civil society organizations, activists, and communities organizing protests against the government.<sup>28</sup> A case in point is the online harassment of Pinappa "Muenoor" Prueksapan, wife of Karen activist Porlajee "Billy" Rakchongcharoen who was disappeared and murdered due to his advocacy for the rights of communities in the Kaeng Krachan National Park, in response to a Facebook post made of her in January 2020. The post was flooded with a large number of negative comments from the accounts of the IOs that denounced Muenoor and despised the Indigenous Karen people.<sup>29</sup> In another Facebook post containing a video of the protest by Indigenous Karen communities of the Kaeng Krachan National Park that took place on 15 February 2021 in front of the UN in Bangkok, comments from the accounts of the IOs stigmatized Karen people and their defenders by referring to them as "aliens from Burma", "Thai person with a Burmese heart" and those who organized rallies to "earn money".<sup>30</sup>

The Vietnamese government has also reportedly been carrying out massive online surveillance as well as monitoring and trolling of individuals deemed critical of the government through "public opinion shapers" such as "Force 47" that act under the authority of the Department of Propaganda since 2013. For example, in January 2020, in course of a land dispute in Dong Tam nearby Hanoi, confrontations between the villagers and the police resulted in deaths of 3 officers and an 84-year-old village leader, which went viral on social media. The government suspended both internet and telephone networks to restrict information sharing and deployed the cyber army of Force 47 to block and counter social media critical of the way authorities handled the situation. Facebook was also seemingly involved in censoring accounts such as in the case of Bui Van Thuan, who received a

---

mobilefordevelopment/resources/mobile-gender-gap-report-2019/; Mia Chung and Pyrou Chung, *Mekong women in open data*, 2020, available at: <https://data.opendevlopmentmekong.net/dataset/mekong-women-in-open-data/resource/74805dc6-d1e8-44a3-8290-e31d5da5f070>

27 Free Expression Myanmar, *Daring to defy Myanmar's patriarchy*, December 2018, available at: <https://freeexpressionmyanmar.org/wp-content/uploads/2018/12/daring-to-defy-myanmars-patriarchy.pdf>

28 Australian Institute of International Affairs, *Are The Thai Army's Information Operations Self-Defeating?*, available at: <https://www.internationalaffairs.org.au/australianoutlook/are-the-thai-armys-information-operations-self-defeating/>; Bangkok Post, *Isoc says 'cyber war' only on fake news*, 28 February 2020, available at: <https://www.bangkokpost.com/thailand/general/1867154/isoc-says-cyber-war-only-on-fake-news>

29 คอมชัดลึก, Facebook post, 25 January 2020, available at: <https://www.facebook.com/komchadluek/posts/10158258701529668>;

30 The Reporters, Facebook post, 9 February 2021, available at: <https://www.facebook.com/TheReportersTH/videos/888345671952642>

company's notification that his posts were violating the Community Standards. Although he tried to appeal the company's decision, Facebook ignored his attempts until the company gave in to civil society pressure. Facebook also restricted the profiles of people attempting to seek more information about the incident. Several land rights activists were arrested for their online activism in relation to the incident and charged under the Criminal Code.<sup>31</sup>



Bunong children is collecting J'yam in their village, Mondulakiri province, Cambodia.

---

31 See Vietnam country chapter below.

# IV. IEHRDs and Cybersecurity laws and policies

## Relevant international declarations, covenants, and other agreements

The Universal Declaration of Human Rights (UDHR) applies to all the Mekong countries as Member States of the UN. The Declaration sets out, among others, the rights to freedom of opinion and expression, including to seek, receive and impart information, and of peaceful assembly and association, which are vital for the works of the IEHRDs. Those freedoms are elaborated in the International Covenant on Civil and Political Rights (ICCPR), which four Mekong States, except Myanmar, are Parties to. The Covenant provides that restrictions may be placed on the exercise of those rights as prescribed by law and needed in the interests of national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others.

However, the Human Rights Committee, its General Comment 34, has noted that the restrictions on freedom of expression “must conform to the strict tests of necessity and proportionality” and that it is not compatible to invoke the laws relating to national security “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 information.”<sup>32</sup> The Committee’s General Comment 37 puts similar requirements for any restriction on the right of peaceful assembly.<sup>33</sup>

All the five States in the Mekong region are Parties to the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), which is described as an international bill of right for women. However, as noted above, women in general, including women IEHRDs, are still facing discrimination than their male counterparts to exercise their rights, including to freedom of expression, in contravention of the Convention.

Further, the UN Declaration on Human Rights Defenders<sup>34</sup> adopted by consensus by the General Assembly in 1998 is applicable to the Mekong States. It identifies human rights defenders as individuals or groups who act to promote, protect or strive for the protection and realization of human rights and fundamental freedoms through peaceful means, and recognizes the key role of human rights defenders in the realization of the human rights enshrined in the UDHR and legally binding treaties and in the international human rights system. It provides for the support and protection of human rights defenders in the context

32 Human Rights Committee, *General comment No. 34 – Article 19: Freedoms of opinion and expression*, 12 September 2011, available at: <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf> <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25397>

33 Human Rights Committee, *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*, 17 September 2020, available at: [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f37&Lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f37&Lang=en)

34 The Declaration’s full name is **Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms**.

of their work and outlines some specific duties of States and the responsibilities of everyone with regard to defending human rights, in addition to explaining its relationship with national laws.

All Mekong States voted in favor of adoption of the UN Declaration on the Rights of Indigenous Peoples at the UN General Assembly in 2007. The Declaration establishes a universal framework of minimum standards for the survival, dignity and well-being of the Indigenous Peoples of the world and it elaborates on existing human rights standards and fundamental freedoms as they apply to the specific situation of Indigenous Peoples. None of the countries has ratified Indigenous and Tribal Peoples Convention, 1989 (No. 169) of the International Labour Organization (ILO), which is the only international treaty dealing exclusively with the rights of these peoples.

## National laws

Constitutions of all Mekong countries recognize the fundamental rights of their citizens or persons, including to freedom of opinion and expression, press, assembly and association, as well as right to access information and to privacy as per their laws. The Thai Constitution also affirms not only the rights of a person but also communities to access public data or information and participation in decision-making affecting them. However, significant restrictions are imposed on those rights in the constitutions or the concerned laws in the name of maintaining national security, interests or unity, public order and morals, protecting the honor or rights of other persons, good customs of society and community peace. For example, in Cambodia, the 2018 constitutional amendments require that individuals and political parties “shall primarily uphold the national interest” and “shall not conduct any activities which either directly or indirectly affect the interests of the Kingdom of Cambodia and of Khmer citizens.” The broad and vague legal restrictions on the exercise of the fundamental rights and their applications to criminalize the legitimate works of IEHRDs and other HRDs in Mekong countries contravene international human rights standards. Some relevant key and representative laws – existing or proposed – in the Mekong countries are discussed below, which are analysed in detail in the respective country chapters in this report.

## Criminal/Penal Codes

The Criminal Codes in Cambodia, Lao PDR, Thailand and Vietnam and the Penal Code in Myanmar include vague and broadly formulated offenses and harsh penalties for those offenses that result in restrictions on freedom of expression (both online and offline), assembly and other fundamental freedoms. Those include provisions related to defamation, libel/slander and/or public insult in the Criminal Codes of Cambodia, Lao PDR and Thailand and in the Penal Code of Myanmar, which are routinely used to target those reporting on human rights abuses at the hands of the State authorities or businesses.

A case in point is the defamation case filed under the Criminal Code by Thailand's public prosecutor and a public official against an Indigenous Karen community leader, Mr. Wuth Boonlert for sharing a post written by a retired national park employee, in which he criticized some government officials for trespassing into a preserved forest area to construct a resort. It was only after long court processes that the Court dismissed the case in November 2019 noting that Wuth's sharing of

the post constituted fair comment on person subjected to public criticism and thus not defamation, which was also upheld by the Court of Appeals in 2020.<sup>35</sup> Also, two IEHRDs and six Karen community members from Omkoi district in Chiang Mai Province were sued by a local mining company for defamation under the Criminal Code for reading out a statement and making a speech against the coal mine at a protest in June 2019.<sup>36</sup> These incidents demonstrate how criminal provisions on defamation are used to curb both online and offline freedom of expression of the IEHRDs, including to harass them and wear them out even through legal proceedings.

In Cambodia's Criminal Code, there are also provisions criminalizing "incitement to commit a felony", which are frequently used against the IEHRDs and others. In December 2019, the provisions were used to charge a journalist Sath Chanbuth, along with allegation of defamation, for releasing a video online in which he interviewed ten Indigenous families about an alleged land dispute in O'Raing district. Chanbuth rejected the allegations when he was summoned at the court and the case is still ongoing.<sup>37</sup>

In Myanmar, the military junta recently introduced new offences, including on knowingly spreading "fake news" in the Penal Code, along with the amendments to the provisions on sedition and high treason. Lao PDR's Criminal Code also contains provisions criminalizing "propaganda against the state"; cooperation of Lao citizens with foreigners or foreign organizations to undermine the independence, sovereignty, territorial integrity or basic political, defense, security, economic or sociocultural interests of the Lao PDR; and organizing or participating in a group for the purpose of protests with the view of causing turmoil that can result in social damage. The government has used such criminal charges, for example, for the detention of three activists, Ms. Lodkham Thammavong, Mr. Soukane Chaithad and Mr. Somphone Phimmason, in 2017 that the UN declared as an arbitrary detention. They were detained for publishing posts on Facebook in which they criticized the government in relation to corruption, deforestation and human rights violations. They were charged with acts of "betrayal towards the nation", "propaganda against the state" and "gathering for the purpose of causing turmoil" under the 2005 Criminal Code and were sentenced for 12, 16 and 20 years in prison respectively.<sup>38</sup>

Similarly, in Vietnam, the provisions on sharing distorted information about the government; inciting, persuading or gathering people for opposing it and disrupting national security; and abuse of democratic freedoms are the most widely used to clamp down on dissent.

Further, the Criminal Codes of Cambodia and Thailand contains provisions on *lèse-majesté*, which are used to criminalize any criticism or opposition of the

---

35 The Columbia Law School Human Rights Institute, *Government of Thailand & Chaiwat Limlikhitaksorn v. Wuth Boonlert & Samak Donnapee*, July 2020, available at: <https://cfj.org/wp-content/uploads/2020/07/Fairness-Report-on-the-Trials-of-Wuth-Boonlert-and-Samak-Donnapee-in-Thailand.pdf>

36 IPHRDs-Thailand, *SLAPP Against IPHRDs at Omkoi District*, 8 April 2020, available at: [https://tlhr2014.com/archives/14207](http://www.eihrdthailand.net/blog/news/รายงานสถานการณ์ละเมิดสิทธิมนุษยชน/ ; TLHR, จากขบวนคัดค้านเหมืองแร่ทองคำสู่การถูกฟ้องคดีปิดปากของแกนนำชาวบ้าน</a>, 25 October 2019, available at: <a href=)

37 Phnom Penh Post, *Mondulkiri reporter questioned for defamation, incitement*, 3 December 2019, available at: <https://www.phnompenhpost.com/national/mondulkiri-reporter-questioned-defamation-incitement>

38 Human Rights Council, Working Group on Arbitrary Detention, *Opinion No. 61/2017 concerning Lodkham Thammavong, Somphone Phimmason and Soukan Chaithad (Lao People's Democratic Republic)*, 15 September 2017, available at: [https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A\\_HRC\\_WGAD\\_2017\\_61.pdf](https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_61.pdf)



monarchy in those countries – more so in Thailand than in Cambodia. Although the *lèse-majesté* law has been used less frequently in Thailand in recent years, critics of monarchy continue to face prison under other laws.<sup>39</sup>

## Laws on Peaceful Assembly and Association

Mekong countries have adopted or are in the process of adopting various laws that place unnecessary and disproportionate restrictions on rights to freedom of peaceful assembly and association, which are concerning for the IEHRDs and other defenders. For example, the 2009 Law on Peaceful Demonstrations in Cambodia provides for stringent requirements of prior notification to the authorities before public demonstrations, caps the maximum number of attendees to two hundred for an impromptu gathering and even allows the authorities to break up or monitor meetings, trainings and protests deemed hostile to the government. Cambodia's draft Law on Public Order released in 2020 even replaces prior notification provision of the Law on Peaceful Demonstrations with prior authorization requirement for "use of public spaces" in the name of maintaining "public order".

Similarly, the 2015 Public Assembly Act of Thailand gives authorities sweeping powers to ban public assemblies on vague and arbitrary grounds. It prohibits public assembly near or in the locations such as royal palaces and residences, the National Assembly, Government House, and the Thai courts. Most problematically, the law imposes criminal penalties for vaguely worded "duties" of both organizers and participants of public assembly, including a duty not to cause "unreasonable inconvenience" to any person. In Vietnam, the 2005 Decree No. 38 bans gatherings outside state agencies and public buildings, as well as all protests deemed to interfere with the political activities or the State or the Party. The Public Security Circular 09/2005/TT-BCA that serves as implementing guidelines to the Decree forbids gatherings of more than five people without prior state approval. The regulations were used to repress the 2018 demonstrations against the Special Economic Zones and Cybersecurity Law drafts in the country.

The 2015 Law on Association and Non-Governmental Organizations in Cambodia and the 2009 Decree on Associations in Lao PDR tighten controls and restrictions of the authorities on the NGOs/CSOs, including community-based organizations. They confer broad and intrusive powers to the governments to regulate the operation of NGOs/CSOs, including through strict inspection and monitoring of their activities and finances, and even suspend their activities for failing to comply with the regulations.

## Information and Media-related laws

While the Mekong countries in their Constitutions guarantee right to access information and freedom of press, the relevant laws and policies are not aligned with those rights. In Vietnam, the Law on Access to Information denies citizens' access to information deemed to be harmful to State interests, national defense and security. At

---

39 Prachatai, *PM says royal mercy stopped use of lèse majesté law*, 16 June 2020, available at: <https://prachatai.com/english/node/8592>; The Reuters, *Explainer: Thailand's lese majeste law*, 4 August 2020, available at: <https://www.reuters.com/article/us-thailand-protests-monarchy-explainer-idUSKCN2501Q1>

the same time, it grants the State authority to punish activists and journalists sharing any information considered critical or defamatory to the State.

In 2016, the Myanmar government proposed a Right to Information Bill, which was considered a step in positive direction to increase government transparency and accountability despite some weaknesses in the bill. However, the bill has not yet been adopted. The Cambodian government has also committed to adopt a Law on Access to Information. However, the draft Law contains a number of shortcomings, such as failure to define the type of information and institutions to which it applies, lack of effective oversight mechanisms with full power granted to the executive branch to resolve appeals for requests for information, and overly broad exceptions to disclosure by public authorities.

On the other hand, in Lao PDR, the State controls over the media with the Media Act 2008 amended in 2016 and the 2015 Decree on Management of Foreign Media, which impose restrictions to ensure strict adherence to and promotion of government policy. The Decree also contains provisions on prior censorship, the requirements on registration and prior approval, as well as obligations of foreign media to abide by the traditions and culture of the Lao PDR. For example, in 2018, following the dam collapse at the Xe-Pien Xe-Namnoy hydropower project that resulted in approximately 7,000 people displaced, 43 people reported dead and 28 missing,<sup>40</sup> the Prime Minister issued a warning letter to all Lao citizens to not believe the misinformation of the foreign media and social media and instead to only trust information shared by state-owned media.<sup>41</sup> A National Investigation Committee was established to analyse the cause of the dam collapse to the government, which later submitted a report but the findings were never released in full to the public.<sup>42</sup>

Likewise, Vietnam's 2016 Press Law states the press to constitute the "voice of the Party, of the State and social organizations" while the 2011 Decree No. 2 authorizes the State to punish journalists and bloggers for various activities and behaviors, including for using a pseudonym to publish. Likewise, the Broadcasting and Television Business Act in Thailand empowers the National Broadcasting and Telecommunications Commission to suspend or revoke the licenses of radio or television operators broadcasting content deemed false, defamatory to the monarchy, harmful to national security or critical of the government.

## Laws related to State of Emergency

Mekong States have used the pretext of combatting the COVID-19 pandemic to further curtail fundamental freedoms, including to expression and assembly. For example, Cambodia adopted the Law on Management of the Nation in a State of Emergency, which grants sweeping powers to the authorities without judicial

---

40 OHCHR, *Joint Letter from Working Group on business, Special Rapporteur on environment, Special Rapporteur on housing, Special Rapporteur on indigenous peoples, Special Rapporteur on internally displaced persons, Special Rapporteur on poverty, Special Rapporteur on water and sanitation to Lao PDR*, 17 April 2020, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25088>

41 Manushya Foundation and AIPP, *Lao UPR Factsheet on Civic Space*, January 2020, available at: <https://www.manushyafoundation.org/lao-pdr-upr-factsheets>

42 OHCHR, *Joint Letter from Working Group on business, Special Rapporteur on environment, Special Rapporteur on housing, Special Rapporteur on indigenous peoples, Special Rapporteur on internally displaced persons, Special Rapporteur on poverty, Special Rapporteur on water and sanitation to Lao PDR*, 17 April 2020, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25088>

oversight on potential abuse. Those powers include surveillance of communication as well as monitoring and control of social media and banning or limiting distribution or broadcasting “information that can cause public panic or turmoil, damage to national security, or confusion about the situation under the State of Emergency”.

In Thailand, the government invoked the 2005 Decree on Public Administration in Emergency Situation, to declare a state of emergency and implement a set of regulations towards combatting the spread of COVID-19. The Decree bans public gatherings or other activities, “which may cause unrest” and led to charges against more than 80 protesters<sup>43</sup> filed under the Decree by October 2020 for participating in youth-led demonstrations, which started in August that year demanding a new constitution, reforms of the monarchy and resignation of the Prime Minister. It has also been invoked to impose broad censorship as it prohibits the sharing of news that is “false or may instigate fear among the people”.<sup>44</sup>

## Cybersecurity laws

With increasing importance and use of information and communication technologies, Mekong countries have adopted or drafted new laws to control the cyberspace. Earlier laws on telecommunications are also used to regulate online communications and other activities. Very often, the laws increase online monitoring and content blocking and punish legitimate online speech. As a result, they threaten the exercise of the rights to privacy, access information, and freedom of expression and restrict the activities of the IEHRDs and other defenders together with the above-mentioned laws.

In **Cambodia**, the 2015 Law on Telecommunications allows for strong governmental control over information and communications technologies. It permits undeclared monitoring by the authorities of any private conversations or correspondence through telecommunications without clear procedures, accountability and judicial oversight. Further, the 2018 Inter-Ministerial Proclamation (Prakas) on Publication Controls of Website and Social Media Processing via the Internet prohibits all publications, news content sharing, written messages, audios, photos, videos, and other means deemed to undermine national defence, national security, relations with other countries, the national economy, public order, non-discrimination and national culture and tradition. It also authorizes the Ministry of Post and Telecommunications of Cambodia to compel the Internet Service Providers in the country to equip internet surveillance tools to easily filter and block any social media accounts or pages deemed illegal.

Moreover, the 2021 Sub-Decree on the Establishment of the National Internet Gateway (NIG Sub-Decree) seeks to create a single internet gateway for all online

- 
- 43 Fortify Rights, *Thailand: Protect Protest Rights, Drop Charges Against Activists*, 23 October 2020, available at: <https://www.fortifyrights.org/tha-inv-2020-10-23/> ; Human Rights Watch, *Thailand: Emergency Decree Pretext for Crackdown*, 15 October 2020, available at: <https://www.hrw.org/news/2020/10/15/thailand-emergency-decree-pretext-crackdown>
- 44 Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFE.net), *Joint Solidarity Statement – Thailand: Stop Digital Dictatorship over Online Freedom*, 25 October 2020, available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_a6ec0138949847db996260c8308b0c0b.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_a6ec0138949847db996260c8308b0c0b.pdf); Prachatai, *Thailand: Stop using emergency powers to restrict the rights of protesters*, 30 June 2020, available at: <https://prachatai.com/english/node/8619>

traffic to filter through before it reaches an end-user. With the NIG, the authorities can block online content and disconnect all network connections that affect safety, national revenue, social order, dignity, culture, tradition and customs, which can result in arbitrary and abusive blocking of online content and networks. It requires selected gateway operators to retain and share personal data such as IP addresses, identification of route traffic, and other information as required for a period of 12 months, which can enable monitoring of user's online activities.

Additionally, Cambodia's draft Law on Cybercrime has raised more concerns about freedom of expression and privacy online. It contains provisions to criminalize spreading false information through information technology that have an "adverse effect" on national security; public health, safety or finances; relations with other countries; and the results of a national election, that incite racial hostility, hatred or discrimination, or cause a loss of public confidence in the government or state institutions. All those vague terminologies such as "national security" and "loss of public confidence" are subject to interpretation by the authorities. It also imposes obligations of "service providers" to store internet traffic data for at least 180 days and penalizes failure to provide such data upon request by the authorities without requirement of judicial oversight.

In **Myanmar**, a draft Cybersecurity Bill first introduced in 2019 was later abandoned. Amid widespread condemnation by local and international groups, the ruling military junta has introduced a new draft, which gives the military control over the internet and data. The draft Bill, though not yet passed, would require "online service providers" to collect and store user data for three years, and provide such data at request. Further, the government may be able to remove any information it deems "misinformation or disinformation", visit the online services' place of business, and be granted access to data and systems for investigation of an alleged threat, fraud, crime, or "cyber incident", or shut down the provider to safeguard public interest – all without any requirement of notice, warrant, or judicial oversight.

Currently, the 2004 Electronic Transactions Law has been primarily used to regulate and control phone and internet users with harsh criminal punishments. The law forbids sending or distribution of "information relating to secrets of the state" online, which has been used to imprison journalists, bloggers and activists – most notably in 2008 to impose sentences of up to 65 years in prison on activists of the 88 Generation Students Group for their role in anti-government rallies.<sup>45</sup> In 2021, without any notice or consultation, the military junta passed amendments to the Law, including many provisions from the draft Cybersecurity bill. The amendments have added a number of new punishments for online activities, including "creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on cyberspace". A chapter on protection of personal information has also been added, which provides exceptions granting authorities broad powers to collect such information for investigations of criminal cases as well as for stability of state sovereignty, public order and national security. At the same time, the junta has also suspended privacy protections under the 2017 Law Protecting the Privacy and the Security of Citizens, which means that authorities can now enter premises, open private correspondence, or intercept electronic communications, among other

---

45 Jonathan Head, *Harsh sentences for Burma rebels*, BBC, 11 November 2008, available at: <http://news.bbc.co.uk/2/hi/asia-pacific/7721589.stm>

things, without a warrant. The law had been amended in 2020 to clarify that the law was intended to protect citizens from intrusions of the government.

Finally, there is the 2013 Telecommunications Law (amended in 2017), which gives Myanmar's Ministry of Transport and Communications significant powers to regulate and supervise telecommunications services to ensure the "stability and security of the country", prevent "harm to security, law, and peace", and for "the benefit of the people". All those terms are not in the law and there are no safeguards in the public interest. In reality, this law has been used to restrict the freedom of online expression of human rights activists. The defamation provision of the Law was used in June 2020 to charge and arrest Htun Htun Oo, a human rights activist for criticizing the military online. The burden of proof under the provision is high, and so especially concerns IEHRDs and other activists.<sup>46</sup> Article 77 of the Law authorizes the Ministry to cut off a telecommunications service in an "emergency" situation, which was used by the government as the basis of the world's longest internet shutdown in Rakhine and Chin States from June-end 2019 to early February 2021 due to "disturbances of peace and use of internet services to coordinate illegal activities".<sup>47</sup> The shutdown meant that humanitarian organizations could not coordinate assistance to those in need in the region, and during the COVID-19 pandemic, some communities have not received information about the public health emergency and thus have limited ability to protect themselves.<sup>48</sup> The Article was also used in March 2020 to block 221 websites, including websites of ethnic news media and of the organizations of human rights defenders, justified in the pretext of dissemination of "fake news" and misinformation about COVID-19.<sup>49</sup>

In **Lao PDR**, the government has approved the 2014 Decree on Internet-Based Information Control/Management, which forbids dissemination and even making comments in support of various restricted content on the internet. Such content includes, among others, any information that persuades or convinces the Lao people to attack against Lao People's Revolutionary Party or the Government; publicizes "false propaganda" to create discrimination against ethnic groups and against the nation; contains edited and other photos that the law of the Lao PDR has prohibited, including "photos discrediting the Lao tradition"; and reveals national, military or other secrets specified in Lao PDR's legislation and regulation. It also stipulates responsibilities of the Internet Service Providers and website managers to ensure that the restricted content is not disseminated and that individuals, legal entities or organizations may be warned, educated, penalized, fined or subjected to criminal charges for violating the Decree depending on the severity of the case. The provisions of the Decree are extremely vague and subject to the interpretation and abuse by the authorities.

The 2015 Law on Prevention and Combating Cyber Crime of Lao PDR identifies activities "causing damages via online social media" as one of the cybercrimes. Such activities include applying "false, misleading and deceptive information" and bringing

---

46 Human Rights Watch, *Dashed hopes, the criminalization of peaceful expression in Myanmar*, 2019, available at: <https://www.hrw.org/report/2019/01/31/dashed-hopes/criminalization-peaceful-expression-myanmar>

47 Telenor Group, *Network shutdown in Myanmar*, 21 June 2019, available at: <https://www.telenor.com/network-shutdown-in-myanmar-21-june-2019/>

48 Human Rights Watch, *Myanmar: End World's Longest Internet Shutdown*, 2020, available at: <https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown>

49 Article 19, *Myanmar: Immediately Lift Ban on Ethnic News Websites*, 2020, available at: <https://www.article19.org/resources/myanmar-immediately-lift-ban-on-ethnic-news-websites/>; Freedom House, *Freedom on the Net 2020: Myanmar*, 2020, available at: <https://freedomhouse.org/country/myanmar/freedom-net/2020>

information that damages “national security, peace, order in society, national culture and fine tradition of the nation” into computer system, which is punishable with three months to three years in prison and fine from 4 to 20 million Kip. The law also provides for general prohibitions such as propagating to destroy or oppose against the political regime in order to cause turbulence. Service providers can also be punished under the law for “providing conditions or facilities for activities of cybercrime”. The Sector of Posts and Telecommunications is designated to monitor, track, advise and prevent emergency incidents and collect statistics. Although the Lao government’s technical ability to monitor internet usage is limited and the authorities do not block access to websites,<sup>50</sup> the existing cybersecurity laws and policies pose a severe risk of surveillance and privacy breach.<sup>51</sup>

In **Thailand**, the Computer Crime Act, officially known as Commission of Computer-related Offences Act, 2007 (amended in 2017) provides the government with unlimited powers to restrict online speech, undertake surveillance and warrantless searches of personal information and data, undermine the right to use encryption and anonymity, and force service providers to facilitate government surveillance and censorship. For example, the Act criminalizes producing and even disseminating “distorted or fake” computer data in a manner to cause damage “to the public”, “the maintenance of national security, public security, national economic security or an infrastructure involving national public interest”, or “which constitutes an offence relating to security of the Kingdom or an offence relating to terrorism under the Penal Code”. It also imposes criminal liability on the Internet Service Providers for such content even without requirement of their intent, which creates an environment of self-censorship. It necessitates them to retain user data for 90 days or allows for warrantless access to user communication. Also, a criminal defamation provision still exists in the law, which penalizes the use of images of another person that have been created, edited, or adapted in a way that “is likely to impair the reputation of such other person or to expose such other person to hatred or contempt”, despite repeated recommendations from the UN to the Thai government to abolish the provision.

Mandated to implement and enforce the Computer Crime Act, the Ministry of Digital Economy and Society, in October 2019, ordered coffee shops, restaurants, and other venues that offer public Wi-Fi to retain the data of users, including names, browsing history, and log files, for at least 90 days.<sup>52</sup> In October 2020, the Ministry ordered to suspend many online media outlets, including Voice TV, Prachatai, The Reporters, and The Standard citing the Act and the Emergency Decree (mentioned above),<sup>53</sup> but the court later lifted the order.<sup>54</sup> The petition website Change.org was also blocked the same month while it is reported that access to the messaging app

50 U.S. State Department, *2019 Country Reports on Human Rights Practices: Laos*, 2019, available at: <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/laos/>

51 See the Lao PDR country chapter below for more information.

52 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020> ; VOA, *Thailand’s Coffee shops told to track, save public Wi-Fi traffic*, 10 October 2019, available at: <https://www.voanews.com/east-asia-pacific/thailands-coffee-shops-told-track-save-public-wi-fi-traffic>

53 Human Rights Watch, *Thailand: Outspoken TV Channel Banned*, 21 October 2020, available at: <https://www.hrw.org/news/2020/10/21/thailand-outspoken-tv-channel-banned>

54 International Federation of Journalists, *Thailand: Court order to suspend online broadcaster revoked*, 23 October 2020, available at: <https://www.ifj.org/media-centre/news/detail/category/press-releases/article/thailand-court-order-to-suspend-online-broadcaster-revoked.html>; Prachatai, *Court lifts suspension orders against Voice TV*, Free Youth, 22 October 2020, available at: <https://prachatai.com/english/node/8863>

Telegram would soon be restricted with the aim to curb the democracy movement.<sup>55</sup> From January to June 2020, Facebook restricted access to 202 items in Thailand in response to reports from the Ministry alleging violations of lèse-majesté law and the Computer Crimes Act.<sup>56</sup> According to Google's transparency report, the government also sent 37 requests from January to May 2020 to remove 1,362 items across various Google services, including YouTube.<sup>57</sup> Such requests are all related to criticism of the government. While Facebook announced legal response to such orders,<sup>58</sup> the Ministry filed a legal complaint against Twitter and Facebook for failure to comply with takedown requests in September 2020, marking the first time in Thailand that the computer crime law was exercised to prosecute the service providers.<sup>59</sup>

Additionally, Thailand's 2019 Cybersecurity Act toughens online monitoring and grants the authorities the power to carry out mass surveillance. It defines "maintaining cybersecurity" as any measure to mitigate the risk of cyber threats that "affect national security, economic security, martial security, and public order in the country" rather than to protect the security of individuals and netizens and to cope with threats posed in the digital space. It allows government agencies formed under the law to collect personal information when there is a deemed cybersecurity risk. Court permission and oversight is only needed for non-critical and critical level cyber threats. For crisis level threats, the authorities can report to the Court after the threat has already been addressed. Private enterprises have reporting obligations with respect to cybersecurity incidents and failure to report or submit risk assessment reports could be subjected to imprisonment and heavy penalty. Moreover, the 2019 National Intelligence Act gives the National Intelligence Agency unrestricted power to obtain any information from government agencies or individuals in the case of "national security" – a term that remains undefined. It also allows the Agency to force the Internet Service Providers to hand over information, including sensitive personal data, whenever it requests. If a government agency or an individual does not provide the information, the Agency has authority to "use any means, including electronic, telecommunication devices or other technologies" to obtain it.

On the other hand, the Personal Data Protection Act contains some progressive provisions to protect personal data. It restricts collection, use, disclosure or tampering of personal data without the consent of its owner, and outlines how businesses can collect, use, or disclose personal information. It also requires obtaining consent specifically from the subject, whose information is being collected, prior to or at the time of collection - either in writing or through electronic means. In addition, the collection of data must be for a lawful purpose and be of direct relevance or

55 BBC, *Thailand blocks Change.org as petition against king gains traction*, 16 October 2020, available at: <https://www.bbc.com/news/world-asia-54566767> ; BBC, *Thailand protests: Authorities move to ban Telegram messaging app*, 19

October 2020, available at: <https://www.bbc.com/news/world-asia-54598956>

56 Facebook Transparency, Thailand, available at: <https://transparency.facebook.com/content-restrictions/country/TH>

57 Google, *Transparency Report Government requests to remove content, Thailand*, available at: <https://transparencyreport.google.com/government-removals/by-country/TH>

58 Prachatai, *Royalist Marketplace returns*, 25 August 2020, available at: <https://prachatai.com/english/node/8748> ; The Reuters, *Facebook says plans to challenge Thai government demand to block group critical of monarchy*, 25 August 2020, available at: <https://www.reuters.com/article/us-thailand-facebook-statement-idUSKBN25L0BR>

59 Bangkok Post, *Govt taking legal action against major social media providers*, 24 September 2020, available at: <https://www.bangkokpost.com/thailand/politics/1990975/govt-taking-legal-action-against-major-social-media-providers> ; The Reuters, *Thailand takes first legal action against Facebook, Twitter over content*, 23 August 2020, available at: <https://www.reuters.com/article/us-thailand-internet-idUKKCN26F0R7>



necessary for the activities of the data controller. Unfortunately, the Act is yet to come into force, which should have happened by April 2020. Nonetheless, it also has a few problematic provisions that can be abused, such as exemptions allowing Parliament and any committee appointed by them as well as the authorities to collect and use data “to maintain state security, including financial security of the state or public safety” and “with respect to the prevention and suppression of money laundering, forensic science or cybersecurity”.

In **Vietnam**, the 2013 Decree on the Management, Provision and Use of Internet Services and Online Information (Decree No. 72) prohibits online information that is deemed to “oppose the State”, “undermine the national security, social order and safety”, “sabotage the great national unity bloc”, as well as information considered to be state secrets, slanderous or defamatory. It mandates internet-based service providers, including social media, to cooperate with the State authorities, notably the Ministry of Public Security and the Ministry of Information and Communications, to delete online content. Offshore internet-based service providers, such as Facebook or Google, are also obliged to locate at least one server in Vietnam and social media companies are required to “register, store and manage personal information of the persons that establish private websites and other information providers on social networks”. An amendment to the decree drafted in April 2020 by the Ministry of Information and Communications, if voted, can impose added restrictions upon companies. The amendment proposes to establish a mechanism for removing illegal content within three hours upon the Ministry’s request, or to block any content presented as journalistic products. It also threatens to expose the personal data and information of social media users, which would considerably increase the risks of harassment and State persecution.

The 2018 Law on Cybersecurity (LOCS), developed directly from the Decree No. 72, raises numerous concerns about sweeping powers to the Vietnamese government to control the cyberspace. The Law strictly forbids developing, posting and sharing of distorted and fabricated information for the purpose of propaganda or defamation. The same applies to information that represents a national security risk, or that may disrupt public order. It also prohibits divulging State secrets - a concept which lacks precise definition under Vietnamese law. Significant obligations are imposed on tech companies and other internet-based service providers. They must comply with requests of the Cybersecurity Taskforce, under the Ministry of Public Security, regarding content takedowns or sharing of users’ data without any stated requirement for a warrant or judicial oversight. The content deemed critical of the government or harmful to national security must be removed within 24 hours – again without any check and balance from the judiciary. Companies are also responsible for the prevention, monitoring and removal of content deemed in violation of the law. Further, they are refrained from providing services to certain individuals, upon the Cybersecurity Taskforce’s requests, if those individuals have shared content deemed in violation of the law. They are required to locate at least one server in Vietnam – a step meant to facilitate government’s access to users’ data. The law makes it unclear whether people charged under it have access to any legal recourse for appeal. Orders by a court or any other independent body are not required for State authorities to penalize companies, which fail to comply with censorship obligations, cybersecurity audits, reporting requirements, obligations to furnish user data or data localization requests.

In line with above laws, the Vietnamese authorities have pressured major companies such as Google, Facebook and Twitter to remove content from their platforms, notably by restricting the internet or shutting it down temporarily. In late 2017, the Minister of Information and Communication declared that Google had “removed 4500 videos containing bad or toxic content from YouTube” out of 5000 deletions requested by Vietnam while Facebook complied with 159 requests of the government regarding the removal “anti-government accounts”. After having experienced a 7-week disruption of its services between April and June 2020, Facebook recorded a 983% increase in compliance with Vietnam’s requests in the first half of 2020.

Additionally, the 2020 Decree No.15 of Vietnam sets out the penalties for violations of regulations imposed on “postal services, telecommunications, radio frequencies, information technology and electronic transactions”. The Decree lists a number of administrative offences, for which both users and internet service providers can be punished. It has been especially used during COVID-19 to fine individuals for misinformation and fake news spread on the pandemic and its handling by the government.



The Bunong Indigenous Peoples affected by the Lower Sesan II Dam project are commemorating their annual festival and vowing not to leave their village, in Stung Treng province, Cambodia.

## V. Recommendations

While the individual country chapters provide specific recommendations as per the national contexts and legal frameworks, below are some broad recommendations that are based on those in the country chapters and can guide actions for mitigating cybersecurity risks for the IEHRDs while ensuring exercise of the right to freedom of expression.

### Recommendations to the Mekong States

1. The States must **ensure that the national legal frameworks align with the international human rights law** in order to guarantee the rights to freedom of opinion and expression, including to access information, and of peaceful assembly and association. That will require them to undertake significant reforms of the relevant laws so as to ascertain that the legal provisions and the restrictions on those rights are in line with international law, specifically with reference to the **General Comments of the Human Rights Committee on freedom of expression and right of peaceful assembly**.

2. The States should **refrain from forcing technology companies and Internet Service Providers to take part in government censorship and surveillance** and require them to respect human rights in line with the UN Guiding Principles on Business and Human Rights.

3. The States should immediately **halt any reprisal against the IEHRDs and other human rights defenders** in online and offline spaces and **redress those that have faced reprisals** for their legitimate works. For that, they should end all ongoing legal proceedings against the HRDs facing charges, investigation or prosecution due to their activism. The States should instead **support and protect them** from non-State actors such as businesses and armed groups **as per the Declaration on Human Rights Defenders**. That should include providing necessary legal protections for the human rights defenders and taking effective actions against State and non-State actors responsible for risks, threats and reprisals against them.

4. The States should **recognize and protect the identities and rights of Indigenous Peoples in their territories** as per the international human rights instruments, including the **UN Declaration on the Rights of Indigenous Peoples**. That will require carrying out legislative and policy reforms, including formulation of new ones; enhancing awareness of the concerned State authorities on the rights of Indigenous Peoples and challenges therefor; as well as enforcing guidelines for implementation of their rights such as for meaningful consultations with the Indigenous communities, including their human rights defenders, to obtain their **Free, Prior and Informed Consent (FPIC)** for decision-making on matters affecting them.

5. The States should **set up or strengthen their judicial and non-judicial grievance mechanisms**, including courts, national human rights institutions, etc., in order to ensure that the violations of human rights of the IEHRDs and the communities they work with are effectively remedied in line with international human rights standards.

## Recommendations to digital technology companies

1. Digital technology companies should **respect the internationally recognized human rights**, regardless of their obligations under the legal frameworks of the States, **in line with the UN Guiding Principles on Business and Human Rights**. For that, the companies should ensure that their policies and terms of service are uniform and comply with the current international standards on freedom of expression and protection of data privacy. They should ascertain that requests/orders to access information with them are legitimate and necessary for a justifiable reason as well as subject to independent oversight. They should also publish regular information on such requests made by the State and other entities as well as the number or percentage of requests they complied with, and about the content or users restricted or removed under the companies' own policies. Further, they should set up effective company-level grievance mechanisms to redress impacts, as they occur, on the rights of IEHRDs that they are responsible for or complicit in, and participate in the State-based mechanisms to increase their accountability.

2. The companies should **cooperate with the IEHRDs and the wider civil society** to increase their awareness on digital tools that can be useful for their works and ensure their security in the cyberspace as well as to develop collaborative technologies that advance human rights.

## Recommendations to project developers and investors

1. **In line with the UN Guiding Principles on Business and Human Rights**, the project developers and investors involved in activities impacting the rights of Indigenous communities should **respect the internationally recognized human rights, including the UN Declaration on the Rights of Indigenous Peoples**, regardless of their obligations under the legal frameworks of the States. That includes conducting **effective impact assessments and human rights due diligence processes** with full information disclosure and meaningful consultations with the concerned communities, including their human rights defenders, to obtain their Free, Prior and Informed Consent (FPIC) for decision-making on matters affecting them. In course of the project implementation, they should take all necessary measures to ensure that their project activities or investments do not cause, contribute or remain complicit in violations of the rights of Indigenous Peoples or the IEHRDs. Additionally, they should establish **grievance mechanisms** – at the institutional and operational levels – to address grievances effectively as they arise and participate in the State-based grievance mechanisms.

2. The project developers and investors should **facilitate partnerships with the Indigenous communities and the IEHRDs** to assist in the realization of human rights-based development in line with the 2030 Agenda for Sustainable Development.

## Recommendations to IEHRDs

1. IEHRDs should increase their understanding of cybersecurity risks through **capacity building in digital literacy** and apply the acquired knowledge and skills to use secure methods of online communication and data storage in order to **minimize and mitigate threats in the cyberspace**. There are various tools and tactics developed by human rights organizations and being used by human rights defenders that can be applied as per the specific contexts of the IEHRDs. They should also strengthen the knowledge of the

communities they work with on the cybersecurity threats using appropriate training methods and materials, including specific measures for women to address their particular needs and challenges.

2. IEHRDs should **identify and document threats** to their works in the cyberspace to use such documentation to bring about change in laws and practices related to cybersecurity. For that, they should **increase their advocacy** with national and international human rights bodies and other relevant mechanisms as well as with the concerned government authorities and business entities. Such engagement should be aimed at holding the authorities and the entities liable for any abuse of the cybersecurity laws resulting in violations of human rights and influencing broader legislative reforms for promotion and protection of the rights of Indigenous Peoples and wider human and environmental rights.



Bunong Youth are showing their unity to protect their ancestral land and natural resources, Mondulkiri province.





Karen activist holding up the banner with the message “stop torture” in Bangkok, Thailand.







# CAMBODIA

Prepared by **Emilie Pradichit**,  
*Manushya Foundation*



# 1. Introduction

## 1.1 Profile of Indigenous Peoples in the country

Map of Distribution of IPs in Cambodia



Source: Open Development Cambodia, <https://data.opendatacambodia.net/dataset/map-indigenous-people-areas-in-cambodia>

Cambodia is a multi-ethnic country with 24 Indigenous communities. With a population of 16.49 million, Indigenous Peoples (IPs) account for 1.4% of the national population (around 400,000 individuals).<sup>60</sup> They mainly live in 15 provinces of Cambodia, including Rattanakiri, Mondulakiri, Stung Treng, Kratie, Preah Vihear, Kampong Thom, and Koh Kong. Their territories include north-east mountainous regions and the mountainous areas in the south-west, making up approximately 25% of the national territory (See map below). The largest Indigenous communities are the Kuy, Phnong, Stieng, Brao, Tampuan, Pear, Jarai and Rade, who mainly speak Mon-Khmer or Austronesian languages. Many of them live a traditional lifestyle, practicing swidden subsistence farming.<sup>61</sup>

60 IWGIA, *Indigenous World 2020: Cambodia*, 11 May 2020, available at: <https://www.iwgia.org/en/cambodia/3599-iw-2020-cambodia.html> ; World Bank, *Total Population-Cambodia*, available at: <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=KH>

61 Minority Rights Groups International, Cambodia, available at: <https://minorityrights.org/country/cambodia/> ; Cambodia Indigenous Peoples Alliance (CIPA), Cambodia Indigenous Youth Association (CIYA), and Asia Indigenous Peoples Pact (AIPP), *Situation of Indigenous Peoples in Cambodia, Submission for the 3rd Cycle of Universal Periodic Review of Cambodia 32nd Session of the Human Rights Council*, 2019, available at: <https://www.ohchr.org/EN/HRBodies/UPR/Pages/UPRKHStakeholdersInfoS32.aspx> ; Minority Rights Group International, *World*

## 1.2 Legal framework on the rights of Indigenous Peoples

In spite of its vote in favor of adopting the UN Declaration on the Rights of Indigenous Peoples (UNDRIP) in 2007 and its ratification of international human rights treaties that reflect principles of UNDRIP, the Cambodian government fails to recognize the rights of Indigenous Peoples in line with those international standards. It refers to Indigenous Peoples as “Indigenous communities”, “Indigenous ethnic minorities” and “highland peoples” in its laws and policies. IPs continue to face discrimination and gradual deterioration of their rights to land and resources.

The Land Law of 2001<sup>62</sup> and the Forest Law of 2002<sup>63</sup> recognize and protect Indigenous Peoples’ rights to use communal land and allow IPs to apply for community land titling (CLT). Nevertheless, the problematic implementation of these laws has been negatively affecting IPs. For example, the process of CLT is lengthy and bureaucratic as noted by the Special Rapporteur on the Rights of Indigenous Peoples and the Special Rapporteur on the Situation of Human Rights in Cambodia in 2017. They have expressed concerns that “complex and costly land titling processes – in which Indigenous Peoples and supporting organisations bear the bulk of the financial costs – are putting Indigenous Peoples in Cambodia at serious risk of losing their traditional lands and resources, in particular sacred forests and gravesites, and their distinct identities as Indigenous Peoples.”<sup>64</sup> As of March 2021, a total of 27 communities held CLTs. Yet only a fragment of communal land is legally recognized and more than 500 Indigenous communities remain without CLTs.<sup>65</sup> Besides, the economic land concessions (ELCs) which the government granted to agro-industrial and mining companies without seeking FPIC from the concerned IPs or providing fair compensation for affected communities create barriers for IPs to enjoy their rights to land as well as the rights to an adequate standard of living, leading to forced evictions and harming their livelihoods and their spiritual and cultural traditions.<sup>66</sup>

National Policy on the Development of Indigenous Peoples, adopted in 2009, seeks to ensure the rights of IPs are safeguarded and livelihoods and quality of life are promoted across all sectors including culture, education and vocational training, health, environment, land, agriculture and water resources, infrastructure, justice, tourism, and industry, mines

---

*Directory of Minorities and Indigenous Peoples - Cambodia : Indigenous peoples*, November 2017, available at: <https://www.refworld.org/docid/5b9b75bf7.html> ; IWGIA, *Indigenous World 2020: Cambodia*, 11 May 2020, available at: <https://www.iwgia.org/en/cambodia/3599-iw-2020-cambodia.html>

- 62 The Land Law, 2001, available at: [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiksenR\\_d7vAhXjIqYKHZegDOAQFjAEegQIAxAD&url=http%3A%2F%2Ffaolex.fao.org%2Fdocs%2Ftexts%2Fcam27478.doc&usg=AOvVaw2z9V6yJMIYTsxiodnrfbFa](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiksenR_d7vAhXjIqYKHZegDOAQFjAEegQIAxAD&url=http%3A%2F%2Ffaolex.fao.org%2Fdocs%2Ftexts%2Fcam27478.doc&usg=AOvVaw2z9V6yJMIYTsxiodnrfbFa) ;
- 63 The Forest Law, 2002, available at: <http://extwprlegs1.fao.org/docs/pdf/cam50411.pdf>
- 64 Special Rapporteur on the rights of indigenous peoples and the Special Rapporteur on the situation of human rights in Cambodia, *Communication No. OL KHM 6/2017, Joint Letter to the Government of Cambodia*, 1 December 2017, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=23484>
- 65 Open development Cambodia, *Registered indigenous communal land*, available at: <https://data.opendevdevelopmentcambodia.net/en/dataset/registered-indigenous-communal-land/resource/ad186575-e436-4a12-a01c-90353261719d>
- 66 Cambodia Indigenous Peoples Alliance (CIPA), Cambodia Indigenous Youth Association (CIYA), and Asia Indigenous Peoples Pact (AIPP), *Situation of Indigenous Peoples in Cambodia, Submission for the 3rd Cycle of Universal Periodic Review of Cambodia 32nd Session of the Human Rights Council*, 2019, available at: <https://www.ohchr.org/EN/HRBodies/UPR/Pages/UPRKHStakeholdersInfoS32.aspx>

and energy. The lead government agency to implement the plan is the Ministry for Rural Development.<sup>67</sup>

The Ministry of Environment has developed an Environment and Natural Resources Code (ENR Code) in 2015 while the final draft (11<sup>th</sup> version) was finalized in 2019 and is now pending adoption.<sup>68</sup> It is expected to be a revolutionary landmark to shape the environmental law framework and address higher levels of environmental protection. With respect to Indigenous rights, the ENR Code is a step in the right direction as it provides for provisions on the principle of FPIC and legal recognition of IPs. Nevertheless, civil society organizations point out that there are loopholes in the legislation. For example, the definition of some terms, including “customary rights”, “customary tenure rights”, or “customary land tenure”, remains vague and requires more clarity and coherence to improve legal recognition of Indigenous claims to land. It was also suggested that the ENR Code emphasises more on the role of affected IPs and communities to be granted sufficient time to make decisions related to their social, cultural, and economic rights and fully participate in all stages of the project development.<sup>69</sup>

While the current laws and policies generally recognize the economic, social and cultural rights of individuals in Cambodia, socio-economic rights of IPs such as the right to education, health services and non-discrimination have long remained challenged. Stemming from poverty, lack of knowledge and education, and inaccessibility of health services in the area, IPs have had poorer health status and experienced a high rate of chronic food infection. The dropout rate among IP children is higher than the rate among the major ethnic group while the literacy rate among IPs is low.<sup>70</sup> With these vulnerabilities, IPs have been increasingly marginalized.

67 Ministry of Rural Development (MRD), *National Policy on the Development of Indigenous Peoples (NPDIP)*, 2009, available at: [https://web.archive.org/web/20190712225752/http://ebooks.libraryrule.com:80/images/pdf\\_file\\_item/a0ef14d817e9190a33e2389e11639c50.pdf](https://web.archive.org/web/20190712225752/http://ebooks.libraryrule.com:80/images/pdf_file_item/a0ef14d817e9190a33e2389e11639c50.pdf); Open Development Cambodia, *Ethnic minorities and indigenous people*, 15 July 2016, available at: <https://opendevdevelopmentcambodia.net/topics/ethnic-minorities-and-indigenous-people/#ref-95458-8>

68 Draft Environment and Natural Resources Code: 11th Draft, 2018, available at: [https://data.opendevdevelopmentcambodia.net/en/laws\\_record/draft-environment-and-natural-resources-code-11th-draft](https://data.opendevdevelopmentcambodia.net/en/laws_record/draft-environment-and-natural-resources-code-11th-draft); Royal Government of Cambodia, *Cambodia's Voluntary National Review 2019 of the Implementation of 2030 Agenda*, June 2019, P.36, available at: [https://sustainabledevelopment.un.org/content/documents/23603Cambodia\\_VNR\\_PublishingHLPF.pdf](https://sustainabledevelopment.un.org/content/documents/23603Cambodia_VNR_PublishingHLPF.pdf)

69 Mongabay, In Cambodia, a sweeping new environment code languishes in legal limbo, 26 August 2020, available at: <https://news.mongabay.com/2020/08/in-cambodia-a-sweeping-new-environment-code-languishes-in-legal-limbo/>; Mekong Region Land Governance (MRLG), *Review, Comments and Recommendations on the Draft Environment and Natural Resources Code (Version 11) of Cambodia*, March 2019, available at: [https://www.mrlg.org/wp-content/uploads/2019/07/Cambodia\\_ENR-Code\\_FINAL.pdf](https://www.mrlg.org/wp-content/uploads/2019/07/Cambodia_ENR-Code_FINAL.pdf); NGO Forum, *Civil Society Organizations' Comments of Draft 11 of the "Environment and Natural Resources Code" of the Kingdom of Cambodia*, 2018, available at: <http://www.ngoforum.org.kh/wp-content/uploads/2018/07/ENR-Code-ENG.pdf>

70 Cambodia Indigenous Peoples Alliance (CIPA), Cambodia Indigenous Youth Association (CIYA), and Asia Indigenous Peoples Pact (AIPP), *Situation of Indigenous Peoples in Cambodia*, 2019, *Submission for the 3rd Cycle of Universal Periodic Review of Cambodia 32nd Session of the Human Rights Council*, 2019, available at: <https://www.ohchr.org/EN/HRBodies/UPR/Pages/UPRKHStakeholdersInfoS32.aspx>

## 1.3 The situation of Indigenous Environmental Human Rights Defenders (IEHRDs)

Due to the lack of respect for Indigenous Peoples' rights and the government's efforts to push for Economic Land Concessions (ELCs), there have been a large number of land dispute cases between IPs, the government authorities and businesses. To defend the rights to lands and the environment of the IPs, IEHRDs and community-based organizations carry out their work through protests and advocacy while they encounter a series of challenges and are often at risk of intimidation, arbitrary detention, harassment and prosecution in Cambodia, which remains one of the most dangerous places for IEHRDs.

The government has a long record of targeting critics of the government and severely restricting access to information, freedom of expression, and freedom of assembly and association. Independent media outlets continue to be hindered by states' control of permits and licenses and targeted for critical reporting, leaving people limited choices but to access information provided by government-affiliated media. Individuals and activists generally practice self-censorship for the fear of investigation and judicial harassment whereas the country repeatedly cites national security to justify restricting criticism of the government and officials. Peaceful protests need to undergo prior notification or authorization, and unauthorized public events and protests such as those related to land disputes can be disrupted and punished by the authority. Non-governmental organizations (NGOs) and grassroots organizations are subjected to stringent registration and monitoring processes. In face of strict controls and lack of judicial independence, victims of human rights abuse often have limited access to remedies.

Digital technologies have opened new space for IEHRDs, who tend to communicate, campaign and advocate online. For example, the Prey Lang Community Network, a loosely structured network of Indigenous Kouy and Khmer villagers, has used a specially designed app with a security component to document illegal logging since 2015. The app allows IEHRDs and villagers to report and record threats, intimidation and violence related to their forest protection activities, combined with relevant data drawn to assess the situation faced by members. In this manner, IEHRDs' work has been and can be extensively facilitated by technologies.<sup>71</sup> Meanwhile, the authority expands its control over the online sphere. The 2015 Law on Telecommunications criminalizes online expression on grounds of national security and permits mass surveillance of online activities. In recent years, there are several vaguely formulated cybersecurity laws and policy either in the legislative process or newly adopted that increase online monitoring, content blocking and punishment for legitimate online expression, threatening the exercise of the rights to privacy, access to information, and freedom of expression. Under the excuse of containing the COVID-19 pandemic, the State of Emergency Law that allows the government to monitor social media and criminalize "fake news" has violated and can further violate online freedom.<sup>72</sup> With the shrinking online space, IEHRDs have become increasingly vulnerable.

71 Prey Lang Community Network (PLCN), *The status of Prey Lang, 7th Monitoring*, 2019, available at: <https://preylang.net/wp-content/uploads/2019/01/7th-Monitoring-Report.pdf>

72 Manushya Foundation, *Spotlight- Restrictive Laws in Cambodia Violating Digital Rights in the Name of "National Security"*, 6 August 2020, available at: <https://www.manushyafoundation.org/post/spotlight-on-restrictive-laws-in-cambodia>

## 2. Methodology

The methodologies used for this report include desk research, interviews and consultations with IEHRDs at local and national levels. Primary sources, including voices, concerns, cases, experiences of IEHRDs, were collected directly from Asia Indigenous Peoples Pact (AIPP) and Manushya Foundation's activities. For example, AIPP organized a regional exchange and training on digital security from 30 September to 2 October 2020, where Indigenous human rights activists from 10 countries participated and shared their experiences with online interference including threats, prosecution, hacking and internet shutdown for their work on Indigenous rights. AIPP carried out analysis of current challenges while Manushya Foundation supported AIPP to assess legal framework and propose recommendations for IEHRDs, and also engaged with Indigenous communities to gain insights and identify human rights violations.

This report is also based on desk research, including a systematic literature review of relevant laws and government regulations; reports and observations/recommendations of United Nations (UN) human rights bodies and NGOs; online news articles; expert papers; and other publications. It aims to present an analysis of the legal framework on cybersecurity laws and potential impacts on IEHRDs.



The Bunong Indigenous men are playing Gong during the commemoration of the annual festival and vowing not to leave their village in Stung Treng province of Cambodia.

### 3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age

**HUMAN DEVELOPMENT INDEX (HDI):** 0.594 (2019)

**NUMBER OF INTERNET USERS IN CAMBODIA:**

8.86 million (as of January 2021)

**LEVEL OF FREEDOM:** 24/100 (with 0 being least free and 100 being most free)

**LEVEL OF PRESS FREEDOM:** 144 of 180 countries

**LEVEL OF FREEDOM ON THE NET:** 43/100 (with 0 being least free and 100 being most free)

**RISK OF CYBERSECURITY THREATS:** 92 of 165 countries (2017 United Nations' International Telecommunications Union Global Cyber Security Index)

**GLOBAL CYBERSECURITY COMMITMENT:** 131 of 175 countries (2018 Global Cyber Security Index)

Cambodia is a practically ruled under a one-party system, dominated by Cambodian People's Party (CPP) and Prime Minister Hun Sen for more than three decades. The fundamental rights of citizens are provided in the Constitution. However, the legislative framework and policies excessively undermine the rights to information, privacy, freedom of expression, association, and peaceful assembly, creating a severely restrictive environment for IPs and IEHRDs, who stand up for their rights. Due to the restrictions imposed on offline activities, a large number of individuals are turning

to internet and social media to express their concerns and seek uncensored information. In January 2021, there were 8.86 million internet users in Cambodia - an increase of 1.1 million (14.4%) between 2020 and 2021. The number of social media users in Cambodia also grew by 2.3 million (23.7%) between January 2020 and January 2021.<sup>73</sup> However, the government has extended its control over the cyberspace by targeting and monitoring online activities through a series of adopted and new draft cybersecurity laws. Legal provisions and policies restricting privacy and criminalizing online expression are continuously invoked to intimidate, investigate, arrest and prosecute individuals peacefully exercising their rights, having a chill effect on IEHRDs and IPs.

#### 3.1 Constitutional provisions stipulating the rights of IEHRDs

The 2008 Constitution of Cambodia affirms a series of rights of Khmer citizens. Article 31 of the Constitution provides for respect for fundamental rights stating that "The Kingdom of Cambodia recognizes and respects human rights as stipulated in the United Nations Charter, the Universal Declaration of Human Rights and the covenants and conventions related to human rights, women's rights and children's rights". It also guarantees that "Khmer citizens shall be equal before the law, enjoying the same rights and freedom and obligations regardless of race, color, sex, language, religious belief, political tendency, national origin, social status, wealth or other status". The rights to freedom of opinion and expression, press, assembly and associations are recognized under Articles 41 and 42 of the Constitution but those rights cannot be abused "to infringe upon the honor of others, or

<sup>73</sup> DataReportal, *DIGITAL 2021: CAMBODIA*, 11 February 2021, available at: <https://datareportal.com/reports/digital-2021-cambodia>



to affect the good customs of society, public order and national security”. Article 40 of the Constitution acknowledges the right to privacy and “the confidentiality of correspondence by mail, telegram, fax, telex and telephone”. Article 39 upholds the right to petition and access to remedy as “Khmer citizens have the rights to denounce, make complaints, or claim for compensation for damages caused by any breach of the law by institutions of the state, social organizations or by members of such organizations. The settlement of complaints and claims for compensation for damages is the responsibility of the courts”.<sup>74</sup> Thus, the Cambodian Constitution enshrines human rights and commits to respecting them in line with international human rights laws. Nevertheless, in 2018, a number of the Constitutional amendments were adopted, which pose a risk to fundamental rights. For example, the amendments require that individuals and political parties “shall primarily uphold the national interest” and “shall not conduct any activities which either directly or indirectly affect the interests of the Kingdom of Cambodia and of Khmer citizens.”<sup>75</sup> With the use of broad terminology in amendments and other restrictive laws, the legitimate exercise of fundamental freedoms is likely to be punished, deterring IPs and IEHRDs from advocating their rights and resulting in marginalization and exclusion.

## 3.2 Legal framework restricting offline activities of HRD

### 3.2.1 The 2014 Criminal Code

#### (A) Defamation, libel and public insult

Articles 305 and 307 of the 2014 Criminal Code<sup>76</sup> criminalize defamation and “public insult”. “Any allegation or charge made in bad faith which tends to injure the honour or reputation of a person or an institution” and “outrageous expression, term of contempt or any invective that does not involve any imputation of fact” in the form of public, written documents, photos, or audio-visual communications released to the public are punishable with a fine of up to 10 million Riels (roughly \$2,500), without a clear definition for the scope of the term “injure”. Defamation in the form of comments made about the government or officials can be charged with “incitement” either “to commit a felony” under Articles 494 and 495 or “to discriminate” under Articles 494 and 496 of the Criminal Code and can be penalized by imprisonment. Article 308 states that an insult committed through the media is subjected to the 1995 Press Law. The Law imposes penalties of up to 5 million Riels on media outlets that post articles, text, pictures, or drawings, which are either false or harm the dignity of an individual.

<sup>74</sup> Constitution of Cambodia, (2008) available at: [https://www.constituteproject.org/constitution/Cambodia\\_2008.pdf?lang=en](https://www.constituteproject.org/constitution/Cambodia_2008.pdf?lang=en)

<sup>75</sup> Fresh News, *Draft Penal Code Amendment related to Lèse-majesté and Constitutional Amendments Promulgated*, 3 March 2018, available at: <http://en.freshnewsasia.com/index.php/en/7748-2018-03-03-05-59-30.html> ; UN High Commissioner for Human Rights (OHCHR), *UN experts say constitutional changes in Cambodia impinge on democracy*, 20 February 2018, available at: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22674&LangID=E>

<sup>76</sup> Criminal Code, 2014, available at: [http://www.sithi.org/admin/upload/law/Criminal\\_Code\\_Book\\_with\\_cover\\_Jan\\_2014.pdf](http://www.sithi.org/admin/upload/law/Criminal_Code_Book_with_cover_Jan_2014.pdf)

**(B) Lèse-majesté<sup>77</sup>**

Article 437-bis of 2018 amendments to the Criminal Code prohibits anyone from defaming, insulting, or threatening the King through “any speeches, gestures, scripts/writing, paintings, or items that would affect the dignity of the King”. Violation can be imprisoned for up to five years and fined up to ten million Riels. The offense also applies to media outlets publicizing, distributing, or circulating, articles, videos, photos, or voice recordings which insult the King.

**(C) “False information” and crime of incitement to commit a felony**

Article 425 of the Criminal Code criminalizes “false information with a view of inducing a belief that a destruction, defacement or damage dangerous to other persons will be carried out”. Communications or disclosing of fake news can be punished with up to 2 years in prison and a fine of up to 4 million Riels. The crime of incitement to commit a felony carried out in public, by writing, pictures, or audio-visual communications, which is frequently invoked, is punishable with a prison sentence of up to 2 years and a fine of up to 4 million Riels under Articles 494 and 495. Individuals whose cases are dismissed as “fake news” can be charged with incitement instead.<sup>78</sup>

These vaguely and broadly formulated offenses in Criminal Codes excessively curb freedom of expression and breach international human rights standards. International standards only allow restrictions on expression provided by law and “formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly”, proportionate, and necessary for “respect of the rights and reputations of others”, “for the protection of national security or of public order, or of public health and morals”.<sup>79</sup>

### **3.2.2 The 2015 Law on Associations and Non-Governmental Organizations (LANGO) and the 2009 Law on Peaceful Demonstrations (LPD)**

The Cambodian government suppresses freedom of peaceful assembly and association and controls civic space through a series of restrictive laws, including LANGO and LPD. Adopted in July 2015, LANGO confers broad and intrusive powers to the government to regulate the operation of NGOs and community-based organizations in Cambodia and even suspend their activities. Registration is mandatory for NGOs and grassroots organizations under Articles 6 and 9(2) while the requirement of “political neutrality” and ministerial discretion over registration in this law are also among major concerns. Organizations are subject to the disapproval of registration applications on broad grounds such as if an organization’s proposed activities jeopardize “peace, stability and public order or harm the national security, national unity, culture, and traditions of the Cambodian national society.” There is no administrative remedy against the rejection of a registration application while

77 Fresh News, *Draft Penal Code Amendment related to Lèse-majesté and Constitutional Amendments Promulgated*, 3 March 2018, available at: <http://en.freshnewsasia.com/index.php/en/7748-2018-03-03-05-59-30.html>; UN High Commissioner for Human Rights (OHCHR), *UN experts say constitutional changes in Cambodia impinge on democracy*, 20 February 2018, available at: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22674&LangID=E>

78 VOD, *Police Witness Talks of Extracting Phone Evidence in Rong Chhun Trial*, 17 February 2021, available at: <https://vodenglish.news/police-witness-talks-of-extracting-phone-evidence-in-rong-chhun-trial/>; RFA, *Cambodian Court Launches Trial of Prominent Union Leader Rong Chhun*, 15 January 2021, available at: <https://www.rfa.org/english/news/cambodia/trial-01152021123456.html>

79 Human Rights Committee, *General comment No. 34*, 12 September 2011, CCPR/C/GC/34, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/453/31/PDF/G1145331.pdf?OpenElement>



unregistered domestic associations and NGOs are banned from carrying out activities and face fines for not complying with the law.<sup>80</sup> Inconsistent with international human rights laws and standards, LANGO poses risks to grassroots movements, community-based organizations and NGOs promoting Indigenous rights and extensively limits their operation and activities.

The LPD, passed in December 2009, places restrictions on freedom of assembly. It includes vaguely worded provisions that require protest organizers to notify the authorities 5 days before the public events and demonstrations or 12 hours before organizing impromptu gatherings on private property or protests at designated venues and limits such gatherings to 200 persons. By law, the government has the power to issue permits for the gatherings and protests after receiving prior notification from the organizers.<sup>81</sup> It allows the government to cite the law to break up or monitor meetings, training programs, protests deemed hostile to the government, curtailing the exercise of the right to freedom of peaceful assembly. IEHRDs and IPs who wish to seek justice through protests and demonstrations are vulnerable under these vague restrictions.

### 3.2.3 The Draft Law on Public Order

Released in August 2020, the draft Law on Public Order<sup>82</sup> contains repressive provisions that criminalize the legitimate exercise of freedom of expression, assembly and association. Article 1 sets out the aim of the law to maintain “public order” by managing “order, aesthetic value, sanitation, cleanliness of the environment, quietness, social stability, preservation of national tradition, and the dignity of citizens”. It encompasses a series of undefined terms leaving them open to interpretation by the authorities. Assembly is further restricted under the draft law as approval from authorities for the “use of public spaces” is required and events with approval can be stopped by authorities, which replaces prior notification principle in LPD with prior authorization requirement. Justifications that can be invoked by the authorities to stop events include broad grounds such as “any hostility with the competent authorities” or “impact to public interests”. Moreover, the number of attendees to events is also regulated in the draft law. These restrictive provisions exacerbate pre-existing difficulties faced by grassroots organizations and Indigenous communities that rely on assemblies to advocate for their rights.

The draft law also raises concerns over freedom of expression – both online and offline. Behaviours such as “speaking loudly”, an expression that impedes “national tradition and dignity”, “exhibiting or disseminating writing or picture or using curse words on social media, showing arrogant behaviour, or disseminating or posting writing signs of pictures that represent any threat”, and even women wearing clothes that are “too short” or “too see-through” that “affect the national tradition and dignity” are prohibited. Violation can result in six days in prison and a fine between 100,000 to 500,000 Riels. If came into effect, the draft law would further be misused and invoked by the authorities to target free speech and hinder the work of IEHRDs.

80 The Law on Associations and Non-Governmental Organizations, 2015, available at: [https://cambodia.ohchr.org/~cambodiaohchr/sites/default/files/Unofficial\\_Translation\\_of\\_5th\\_LANGO\\_ENG.pdf](https://cambodia.ohchr.org/~cambodiaohchr/sites/default/files/Unofficial_Translation_of_5th_LANGO_ENG.pdf)

81 The Law on Peaceful Demonstrations, 2009, available at: [https://cambodia.ohchr.org/sites/default/files/Law\\_on\\_peaceful\\_demonstration-promulgated\\_Eng.pdf](https://cambodia.ohchr.org/sites/default/files/Law_on_peaceful_demonstration-promulgated_Eng.pdf)

82 CSO Joint Statement, *Civil Society Organizations Call for the Draft Law on Public Order to be Immediately Discarded*, 13 August 2020, available at: [https://www.hrw.org/sites/default/files/media\\_2020/08/200813%20CSO%20Joint%20Statement\\_ENG.pdf](https://www.hrw.org/sites/default/files/media_2020/08/200813%20CSO%20Joint%20Statement_ENG.pdf)

### 3.2.4 The 2020 Law on the Management of the Nation in a State of Emergency

Under the pretext of combating the COVID-19 pandemic, Cambodia passed the Law on the Management of the Nation in a State of Emergency (State of Emergency Law)<sup>83</sup>. It grants sweeping power to the government authorities to restrict and prohibit “movement, free speech and business activities, closing public and private spaces”, surveil communication as well as monitor and control social media, and ban or limit “distributing or broadcasting information that can cause public panic or turmoil, damage to national security, or confusion about the situation under the State of Emergency”. It is also concerning that surveillance by “any means” of digital information is also permitted under the law. Punishment for violating the law includes 5 years in prison and a fine of up to 5 million Riels. There is no judicial oversight or any limitation in place that can restrain authorities from abusing the law. With vaguely formulated offenses and broad discretion of the authorities, the law constitutes another tool for the government to stifle critical speech, hinder assembly and target HRDs.

## 3.3 Cybersecurity Laws and policies restricting online activities of IEHRDs

### 3.3.1 The Draft Law on Cybercrime

Cambodia’s draft Law on Cybercrime<sup>84</sup>, after ten years of drafting, was leaked in 2020, which has raised concerns about online privacy and free expression. Although the aim of the cybercrime law is to regulate key issues such as child pornography, identity theft and computer-related forgery crimes, it is one of those broadly and vaguely formulated laws that can be used to undermine online freedom and exacerbate digital dictatorship. Article 45 stipulates up to three years in prison for “false statements or disinformation through information technology” that have an “adverse effect” on national security; public health, public safety, or public finances; relations with other countries; and the results of a national election, that incite racial hostility, hatred or discrimination, or cause a loss of public confidence in the government or state institutions. The lack of clarity of the provision renders the public unable to understand the law or comply with it. Similarly, Article 40 vaguely prohibits acts of “disturbing frightening, threatening, violating, persecuting, or verbally abusing others by means of a computer”, and makes violations of the Article punishable with six months in prison. Both Articles provide the authorities with a broad and subjective interpretation of what constitutes “national security”, “public safety” or “loss of public confidence in the government or state institutions” under the law.

The draft law also imposes the obligations of “service providers” without clarifying the kinds of service providers that come under the scope of this law. Articles 8 and 12 require service providers to store internet traffic data for at least 180 days. Failure to preserve or provide such data upon request by the authorities can be punished with fines and prison sentences. There is no judicial oversight required. The mandatory data retention fails to conform to international human rights standards, which provide that access to and use of data should be tailored to specific legitimate aims and that retaining data “just in case” it

83 Law on the Management of the Nation in a State of Emergency, 2020, available at: <https://akp.gov.kh/post/detail/29564>

84 Human Rights Watch, *Cambodia: Scrap Draft Cybercrime Law*, 13 November 2020, available at: <https://www.hrw.org/news/2020/11/13/cambodia-scrap-draft-cybercrime-law>

is needed for government purposes or for subsequent law enforcement and intelligence agency access is neither proportionate nor necessary.<sup>85</sup> This allows for an intrusion on privacy through potential mass surveillance.

### 3.3.2 The Sub-Decree on the Establishment of the National Internet Gateway (NIG Sub-Decree)

On 16 February 2021, the Cambodian Government issued Sub-Decree No. 23 on the Establishment of National Internet Gateway (NIG Sub-Decree)<sup>86</sup>, which seeks to create a single internet gateway for all online traffic to filter through before it reaches an end-user. The NIG Sub-decree requires internet service providers in Cambodia to reroute their services through the National Internet Gateway (NIG) before February 2022. It provides the government with unlimited power to censor online content, undertake surveillance, intercept personal communication, information and data, and compel gateway operators to facilitate state surveillance, thus undermining the right to privacy, information, and freedom of expression.

With the NIG, the authorities can block online content and disconnect “all network connections that affect safety, national revenue, social order, dignity, culture, tradition and customs”. As the justifications are vague and broad, the blocking of online connections or contents can be arbitrary and abusive. Moreover, it allows the authorities to require selected gateway operators to retain and share personal data such as IP addresses, identification of route traffic, and “other information as required” for a period of 12 months. That can enable the authorities to monitor users’ online activities and identify specific users. In the absence of data protection law in Cambodia, it remains unknown whether the misuse of data can be prevented and how long the government can retain the data and for what purpose, allowing for illegal interference with privacy. Thus, the NIG Sub-decree creates a repressive environment and generates self-censorship among online users and activists.

### 3.3.3 The Draft Law on Access to Information

The Cambodian government has committed to adopt a law promoting access to information, which is in the right direction. That will ensure that citizens have access to all pieces of information held by national and subnational bodies, including information in all official documents under the possession of public institutions. Despite the positive commitment, the draft Law on Access to Information<sup>87</sup> has a number of shortcomings. Those include failure to define the type of information and institutions to which it applies, lack of effective oversight mechanisms and of addressing a presumption of full disclosure, full power granted to the executive branch to resolve appeals for requests for information, overly broad categories of exceptions to disclosure by public authorities, and undefined term “public interest”. It is concerning that the draft law also contains several provisions restricting free expression. For example, “whoever makes a lying denunciation to any public

85 Human Rights Council, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, 30 June 2014, A/HRC/27/37, paras. 23, 26 available at: [https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37\\_en.pdf](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf)

86 LICADHO, *Joint Statement, CSOs call on the Royal Government of Cambodia to repeal the sub-decree on the establishment of the National Internet Gateway*, 19 February 2021, available at: <https://www.licadho-cambodia.org/pressrelease.php?perm=471>; Prashanth Parameswaran, “What’s in Cambodia’s New Internet Gateway Decree?” *The Diplomat*, 24 February 2021, available at: <https://thediplomat.com/2021/02/whats-in-cambodias-new-internet-gateway-decree/>

87 Article 19, *Cambodia: Analysis of the Draft Law on Access to Information*, 10 December 2019, available at: <https://www.article19.org/resources/cambodia-analysis-of-the-draft-law-on-access-to-information/>.

institutions or judicial authorities about an offence, causing the investigation to become useless” is punishable by imprisonment up to 6 months and a fine of up to 1 million Riels.

### 3.3.4 The 2015 Law on Telecommunications

Another repressive law that allows for increased governmental control over information and communications technologies is the 2015 Law on Telecommunications<sup>88</sup>. It permits undeclared monitoring by the authorities of any private conversations or correspondence via telecommunications without clear procedures, accountability and judicial oversight. With this law, the Ministry of Post and Telecommunications of Cambodia (MPTC) is granted sweeping powers to require customers’ personal information and data from “all telecommunications operators and persons involved with the telecommunications sector” without a court warrant under Article 6. The MPTC and other ministries can order internet service providers (ISPs) to take “necessary measures” in cases of force majeure without a clear definition of “force majeure” and the scope of “necessary measures”. Moreover, the law established “telecommunications inspection officials” to enforce the law by investigating alleged offenses, with the ability to call in support from the armed forces. Online activities are criminally liable in many cases. For example, the establishment, installation, and utilization of equipment in the telecommunications sector that “lead to national insecurity” is criminalized under this law and can be punished with up to 15 years in prison or fine of up to 300 million Riels. The term “national insecurity” is undefined and open to potential abuse by the authorities to target online speech critical of the government.

### 3.3.5 Inter-Ministerial Proclamation (Prakas) on Publication Controls of Website and Social Media Processing via the Internet

The Inter-ministerial Proclamation (Prakas) on Publication Controls of Website and Social Media Processing via Internet<sup>89</sup> is a regulation issued by the Ministry of Interior, the MPTC and the Ministry of Information in May 2018. The Prakas prohibits all publications, news content sharing, written messages, audios, photos, videos, and other means deemed to undermine national defence, national security, relations with other countries, the national economy, public order, non-discrimination and national culture and tradition. It specially targets website publications and any kind of online social media networks. Pursuant to the law, the Ministries shall establish specialized units to cooperatively monitor illegal activities and publications on websites and social media in order to take legal action against them. Moreover, the MPTC has the authority to compel ISPs in Cambodia to install software programs and equip internet surveillance tools to easily filter and block any social media accounts or pages deemed illegal. Thus, vague justifications such as “national security”, “political and social stability”, “turmoil”, “national economy” and “breaking solidarity” for prohibitions on website and social media as well as the significant level of the discretion conferred on the authorities to monitor and enforce such prohibitions constitute an undue intrusion on the rights of online users to privacy and freedom of expression.

88 The Telecommunications Law, 2015, available at: [http://www.sithi.org/admin/upload/law/20150127\\_TelecommunicaitonDraftLaw\\_En%20edited-2.pdf](http://www.sithi.org/admin/upload/law/20150127_TelecommunicaitonDraftLaw_En%20edited-2.pdf)

89 Inter-Ministerial Prakas on Social Media Processing via the Internet in the Kingdom of Cambodia, 2018, available at: <https://cyrilla.org/ar/document/7damc09w824?page=3>.

## 4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases

### 4.1 Strategic lawsuit against public participation (SLAPP), threats and harassment for online activity

In the absence of clearly defined offenses and precise terminology, repressive cybersecurity laws and policies in Cambodia disproportionately and excessively criminalize legitimate online expression in the name of “national security”, “political and social stability”, “turmoil”, “national economy” and “breaking solidarity” and “false information” in contravention of international human rights laws. Individuals can be punished with years in prison and fines in connection with online expression under various charges. Accordingly, the government continues to crack down on online dissent and target HRDs by initiating SLAPP cases, summoning and investigating activists, and intimidating and harassing online users.<sup>90</sup> Other powerful actors, such as officials and big companies, are also involved in these actions to silence critics. For the fear of reprisal, self-censorship is widespread among HRDs and ordinary users. Therefore, the ability of IEHRDs to use online platforms for advocacy and seek justice has been diminished.

#### **Case of Kroeung Tola, who was charged with defamation for a Facebook post<sup>91</sup>**

In January 2021, Kroeung Tola, an ethnic Bunong IEHRD, was charged with defamation and ordered to pay 40 million Riels (equivalent to \$10,000) in compensation to O’Raing district governor Siek Mony and four million Riels to the State. He was charged because of his Facebook post, in which he claimed that the governor was involved in the clearing of the 300ha of protected forest in O’Raing district. Tola announced that he was planning to appeal the court decision.

#### **Case of a Bunong activist, who repeatedly received threats<sup>92</sup>**

A Bunong activist from Monduliri province, who is a coordinator of the Indigenous Networking Group, has reported to receive an array of anonymous intimidation and threats of arrest by the district police for his commitment to protect IP rights and the forest. He started engaging in IP rights activities in 2015 and is one of the most proactive activists at the community level. He has experience in advocating on various issues such as land concessions, environmental degradation, and extraction of forest, oil and mineral resources. He frequently uses social media to disseminate information and raise awareness of these issues. Threats and intimidation have had mental and economic effects on him and his family.

90 Manushya Foundation, *Spotlight- Restrictive Laws in Cambodia Violating Digital Rights in the Name of “National Security”*, 6 August 2020, available at: <https://www.manushyafoundation.org/post/spotlight-on-restrictive-laws-in-cambodia>

91 Phnom Penh Post, *Soth Koumsoeun, ‘Activist hit with \$10k defamation fine*, 21 January 2021, available at: <https://www.phnompenhpost.com/national/activist-hit-10k-defamation-fine>

92 IWGIA, *Indigenous peoples in Cambodia: 2019*, 24 April 2019, available at: <https://www.iwgia.org/en/cambodia/3420-iw2019-cambodia.html>

### Case of judicial harassment of Sat Chanbut for interviewing IP families<sup>93</sup>

Sath Chanbuth, a journalist for Rasmei Kampuchea and Apsara TV, was summoned to appear in the Mondulkiri provincial court on allegations of incitement and defamation in December 2019. The lawsuit came after he released a video online, in which he interviewed 10 Indigenous families of O'Raing district's Dak Dam commune about an alleged land dispute. Chanbuth rejected the allegations. The case is still ongoing to date.

### Case of detention of three EHRDs from Mother Nature Cambodia<sup>94</sup>

Mother Nature Cambodia is an environmental rights organisation known for publishing online videos to advocate and campaign for the preservation, promotion and protection of the environment and challenge the government and private interests over development projects. Three EHRDs, Thun Ratha, Long Kunthea and Phuong Keorasmey of the Mother Nature Cambodia were arrested in September 2020 after Long Kunthea posted a Facebook message planning a one-person march from Wat Phnom to the Prime Minister's residence to call for an end to the exploitation of the Boeung Tamok Lake. They were charged with "incitement to commit a felony or cause social unrest". The Ministry of Interior later issued a statement, claiming Mother Nature Cambodia "caused chaos in society". On 20 October 2020, their bail requests were denied by the Court of Appeal in Phnom Penh. To date, they await trial in detention. If convicted, they face up to two years in prison.

## 4.2 Limited access to information caused by restrictions on online content

The recent years have seen deterioration in right to access information online as the government imposes regulations and invokes repressive cybersecurity laws to block access to websites and take down online content. Independent news outlets and other websites continue to be blocked and have their licenses revoked for disseminating criticisms of the government. Before the national elections in 2018, 17 news websites were temporarily blocked for 48 hours due to alleged "provocative" and "very political" news coverage.<sup>95</sup> Amid the COVID-19 pandemic, Monoroom.info, a Khmer-language news website based in France was blocked in March 2020 for reporting on the COVID-19 situation.<sup>96</sup> In 2020, several media licenses were revoked, including for TVFB, CKV TV Online, 99.75 FM Radio and the associated Rithysen news site.<sup>97</sup> There are reports of individuals made to take down content after pressure from the police.<sup>98</sup> The continuous suppression of dissenting voices extensively hinders the right to access information. Content manipulation by the authorities

93 Phnom Penh Post, *Mondulkiri reported questioned for defamation, incitement*, 3 December 2019, available at: <https://www.phnompenhpost.com/national/mondulkiri-reporter-questioned-defamation-incitement>

94 RFA, *Cambodian Civil Society Calls For End to Harassment, Arrests of Mother Nature Youth Activists*, 3 February 2021, available at: <https://www.rfa.org/english/news/cambodia/activists-02032021173152.html>; Frontline Defenders, *Three Environmental Rights Defenders Arbitrarily Detained*, available at: <https://www.frontlinedefenders.org/en/case/three-environmental-rights-defenders-arbitrarily-detained>

95 Committee to Protect Journalists, *CPJ condemns pre-election news censorship in Cambodia*, 30 July 2018, available at: <https://cpj.org/2018/07/cpj-condemns-pre-election-news-censorship-in-cambo/>

96 Reporters without Borders, *Cambodia: Hun Sen uses Covid-19 crisis to tighten his grip*, 9 April 2020, available at: <https://rsf.org/en/news/cambodia-hun-sen-uses-covid-19-crisis-tighten-his-grip>

97 Voice of Democracy (VOD), *News Site Blocked, Journalist Jailed After Quoting Hun Sen*, 9 April 2020, available at: <https://vodenglish.news/news-site-blocked-journalist-jailed-after-quoting-hun-sen/>; VOD, *Journalist Jailed, Media License Revoked Over 'Exaggerated' Coverage*, 15 May 2020, available at: <https://vodenglish.news/journalist-jailed-media-license-revoked-over-exaggerated-coverage/>; Freedom House, *Freedom on the Net: Cambodia*, 2020, available at: [https://freedomhouse.org/country/cambodia/freedom-net/2020#footnoteref3\\_890of4y](https://freedomhouse.org/country/cambodia/freedom-net/2020#footnoteref3_890of4y)

98 Phnom Penh Post, *Rapper Deletes Song Critical of Cambodian Social Issues*, 20 May 2019, available at: <https://www.phnompenhpost.com/national/rapper-deletes-song-critical-cambodian-social-issues>

also exerts interference with the flow of information. Reportedly, there were coordinated cybertroop teams manipulating Twitter for government agencies.<sup>99</sup> More concerning, the intended creation of a single point of entry for internet traffic stipulated in the NIG Sub-Decree increases the government's ability to block online content and limit internet access. Consequently, IEHRDs and IPs, who use the internet as the main sources of news and information, have been increasingly facing barriers to access uncensored information and hold the authorities accountable for harmful development projects and land grabbing.

## 4.3 Invasion of privacy through surveillance and monitoring

The government actively monitors public activities online and carries out extralegal surveillance of private communications using flawed cybersecurity laws. Under the guise of national security, the 2015 Law on Telecommunications grants the government sweeping powers to secretly monitor online activities, emails and private correspondence between individuals without their knowledge or consent and to punish violations when there is a perceived security threat. The 2018 Inter-ministerial Proclamation Prakas expands its surveillance power by requiring ISPs to install surveillance software to monitor online content. The newly passed State of Emergency Law provides the authority with increased power to monitor public and private online discussions and communications. A series of draft cybersecurity laws reinforce the authority conferred on the government to carry out surveillance and monitoring. Without a judicial warrant or procedural safeguards, the laws place no limits on state surveillance.

Moreover, the government has indicated the existence of ongoing online monitoring several times. In 2017, the National Police claimed that they were monitoring Facebook to prevent "rebel movements against the government."<sup>100</sup> As reported in October 2019, the information technology department of the Ministry of Interior planned to set up a Security Operation Center to monitor all digital platforms in order to deter "online threats".<sup>101</sup> Mass surveillance and monitoring not only invade online users' privacy, but also allow for the misuse of this power to subsequently charge IEHRDs for other crimes such as defamation and incitement to commit a felony on the basis of their online advocacy and speech.

## 4.4 Limited access to remedy

Cambodia's cybersecurity laws fail to specify any rights to challenge a decision made by the government authorities or any judicial recourse for victims whose rights are abused when implementing the laws. That exacerbates the pre-existing vulnerabilities of IEHRDs and IPs to human rights violations. Although people have the right to file complaints and petitions under the Constitution, individuals are deterred from seeking judicial remedies due to lack

99 Oxford Internet Institute (OII), *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, September 2019, available at: <https://demtech.oii.ox.ac.uk/research/posts/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/#continue>

100 Phnom Penh Post, *Cambodia's Facebook crackdown: Police are monitoring site for 'enemies' and 'rebel movements'*, 25 July 2017, available at: <https://www.phnompenhpost.com/national/cambodias-facebook-crackdown-police-are-monitoring-site-enemies-and-rebel-movements> ; Phnom Penh Post, *Defence Ministry monitoring Facebook for feedback*, 14 February 2018, available at: <https://www.phnompenhpost.com/national/defence-ministry-monitoring-facebook-feedback>

101 Khmer Times, *Planned security centre raises rights concerns over internet surveillance*, 10 October 2019, available at: <https://www.khmertimeskh.com/50649622/planned-security-centre-raises-rights-concerns>



of trust on the judicial mechanisms due to corruption in and political control over them.<sup>102</sup> In light of restrictions imposed on civil society, organizations can be prevented from effectively advocating on behalf of those affected, leaving IPs and IEHRDs few avenues for redress.



The Bunong youth are preparing for art performance at Orang district of Mondulkiri, Cambodia.

102 U.S. State Department, *Cambodia 2020 Human Rights Report*, 30 March 2021, available at: <https://www.state.gov/wp-content/uploads/2021/03/CAMBODIA-2020-HUMAN-RIGHTS-REPORT.pdf>



## 5. Recommendations

### 5.1 Recommendations to the government

**5.1.1.** Decriminalize online speech and ensure the internet as a free space of expression in line with international human rights laws, including Article 19 of UN Declaration on Human Rights and of the ICCPR; enact a stand-alone anti-SLAPP law to ensure legal protection against SLAPP.

**5.1.2.** Revise existing and draft laws and policies to provide clearer terms and definitions so as to ensure IEHRDs and IPs can fully enjoy their right to free expression without fear of prosecution or self-censorship. This includes amending or repealing the draft Law on Public Order, State of Emergency Law, the draft Law on Cybercrime, the 2015 Law on Telecommunications, the Prakas, the Criminal Code, as well as the relevant provisions in the Constitution.

**5.1.3.** Guarantee all the population access to information as noted in the report of the Special Rapporteur on the situation of human rights in Cambodia (2019). This includes promoting independent media, particularly online media, repealing the NIG Sub-Decree and revising the draft Law on Access to Information.

**5.1.4.** Refrain from forcing tech companies as well as ISPs from taking part in government censorship and surveillance and permit them to comply with their responsibilities to respect human rights in line with the UN Guiding Principles on Business and Human Rights (UNGPs).

**5.1.5.** Release all activists detained for exercising their right to freedom of expression and end all legal proceedings or investigations against them; provide effective remedy, including compensation, for unlawful violation of their rights.

**5.1.6.** Begin the process of establishing a national human rights institution with a mandate to protect the full range of human rights and provide grievance mechanisms in full compliance with the Paris Principles.

**5.1.7.** Provide remedies for loss of livelihoods, environmental damage and land degradation taking into account IPs' traditional lifestyles, including fair and adequate compensation, which have occurred due to various ELCs and other development projects.

**5.1.8.** Remove barriers to access effective judicial remedies for IPs through courts, including by providing effective interpretation and free legal aid services; ensure prompt investigation into complaints filed against development projects, state authorities, law enforcement officials and companies; tackle corruption and the lack of transparency and independence in the judiciary.

**5.1.9.** Require free, prior and informed consent of IPs prior to any project affecting their lands, territories and resources in line with international human rights standards, including through enforcement of National Policy on the Development of Indigenous Peoples and adoption of necessary new laws and policies.

### 5.2 Recommendations to digital technology companies

**5.2.1** Ensure the companies' terms of service and policies are uniform and comply with international standards on freedom of expression and protection of data privacy, which are reviewed regularly to ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological and societal developments in line

with the obligation to respect human rights under the UNGPs.

**5.2.2.** Ensure that any requests, orders and commands to access information are based on validly enacted law, subject to external and independent oversight, and demonstrates a necessary as well as proportionate means to achieve one or more aims.

**5.2.3.** Publish regular information on their official websites regarding the legal basis of requests made by governments and other third parties and regarding the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own policies and community guidelines.

**5.2.4.** Provide company-level remedies and grievance redress mechanisms – both physical and virtual – to victims affected by adverse impacts of cybersecurity responses that violate their rights.

**5.2.5.** Collaborate with the government and civil society to develop technology that promotes and strengthens human rights.

## 5.3 Recommendations to project developers and investors

**5.3.1.** Take all necessary and lawful measures to ensure that business practices do not cause, contribute or remain complicit in violations, with respect to the rights of IPs and IEHRDs.

**5.3.2.** Facilitate partnerships of companies with IPs and IEHRDs to assist in the realization of the UNGPs and Sustainable Development Goal (SDG) commitments.

**5.3.3.** Conduct assessments and due diligence processes to determine the impact of business activities on IPs with respect to individual and community rights; ensure full participation by and consultation of the affected IPs and EHRDs.

**5.3.4.** Disclose information related to planned and ongoing large-scale development projects in a timely and accessible manner to the affected communities and IEHRDs.

**5.3.5.** Establish and participate in effective non-State-based grievance mechanisms, including at operational levels.

## 5.4 Recommendations to IEHRDs

**5.4.1.** Engage in the process of understanding digital threats to civic space; identify and document internal and external threats to the rights of expression with respect to the legal framework.

**5.4.2.** Use encrypted communication in daily works, choose online platforms that allow users to send encryption-protected information to others and collect and store very little data about users to mitigate surveillance.

**5.4.3.** Ensure that the software versions are up to date and authentication inside and out is upgraded.

**5.4.4.** Increase engagement with business and the government in support of Indigenous rights and digital rights; provide recommendations on the implementation of cybersecurity laws and laws regarding IPs.

**5.4.5.** Hold implementing authorities and officials liable for the misuse of their powers or information obtained while carrying out their duties under cybersecurity laws.



A photograph of a person wearing a traditional conical hat and dark clothing, standing in a river and using long wooden poles to fish. The person is positioned in the lower right foreground, with their body angled towards the left. The water is calm and reflects the light. In the background, another person is visible in a small boat on the river, and a shoreline with some vegetation and buildings is visible in the distance. The overall scene is peaceful and depicts a traditional fishing method.

# Lao PDR

Prepared by **Emilie Pradichit,**  
*Manushya Foundation*

# 1. Introduction

## 1.1 Profile of Indigenous Peoples in the country

The Lao People's Democratic Republic (Lao PDR) or Laos is the most ethnically diverse country in Southeast Asia. The concept of "Indigenous Peoples" (IPs) is not recognised. Instead, the government uses the term "ethnic groups" to refer to Indigenous Peoples. With a population of 7 million, 240 subgroups are recognized within 50 official ethnic groups, which are categorized into one of four ethnolinguistic groups: Lao-Tai (that makes up 62.4 percent of national population), Mon-Khmer (23.7 percent), Hmong-lu Mien (9.7 percent), and Sino-Tibetan (2.9 percent).<sup>103</sup> While the Lao-Tai speaking groups dominate politically, culturally and economically, the last three groups which account for one-third of the total population are considered as the Indigenous Peoples of Laos and practice more traditional ways of life.<sup>104</sup>

The Lao-Tai ethnolinguistic group is composed of eight individual ethnic groups that reside in lowland areas in the Mekong Valley and its outlying areas. The first inhabitants of the modern-day Laos territory are the Mon-Khmer family made of 33 individual ethnic groups.<sup>105</sup> The Hmong-Mien family comprises of two ethnic groups, who mostly reside in the northern area. The seven other groups belonging to the Sino-Tibetan family traditionally inhabit the uplands of Laos<sup>106</sup> (see table below). Buddhism is the most prevalent religion among Lao-Tai groups while non-Lao-Tai groups are mostly animist.<sup>107</sup>

Officially, these groups are categorized into three broader groupings by the government on the basis of the geographic areas: Lao Loum who live in the lowlands around the fertile river deltas; Lao Theung live in the middle-altitude lands who have been experiencing discrimination by other groups; and the highland groups, Lao Sung who are traditionally quite isolated from the mainstream.<sup>108</sup> These categories tend to promote unity and the commonality of the nation, which overlooks diversity, and cultural and economic differences among ethnolinguistic families.

103 Open Development Laos, *Ethnic minorities and indigenous people*, 3 June 2019, available at: <https://laos.opendevdevelopmentmekong.net/topics/ethnic-minorities-and-indigenous-people/>

104 IWGIA, *Indigenous World 2020: Laos*, 11 May 2020, available at: <https://www.iwgia.org/en/laos/3604-iw-2020-laos.html>

105 AIPP, IWGIA, *Indigenous Peoples in ASEAN: Lao PDR*, 2015, available at: [https://aippnet.org/wp-content/uploads/2020/02/15.-Asean-study\\_Laos\\_15\\_July\\_2015\\_Final\\_PM.pdf](https://aippnet.org/wp-content/uploads/2020/02/15.-Asean-study_Laos_15_July_2015_Final_PM.pdf)

106 Open Development Laos, *Ethnic minorities and indigenous people*, 3 June 2019, available at: <https://laos.opendevdevelopmentmekong.net/topics/ethnic-minorities-and-indigenous-people/>

107 Minority Rights Groups International, Laos, available at: <https://minorityrights.org/country/laos/>

108 Christopher Muscato, Study.Com, *Laos Ethnic Groups*, available at: <https://study.com/academy/lesson/laos-ethnic-groups.html>

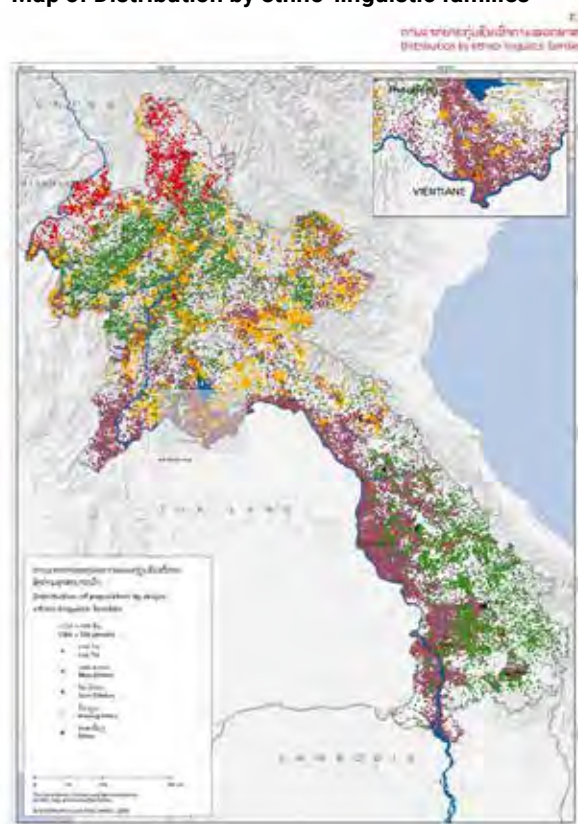
**Table:** Ethno-linguistic Families, Ethnic Groups, and Demographic Information

Ethno-linguistic Family	Number of Ethnic Groups	Percentage of National Population	Territories
Lao-Tai	8	62.4	Mekong Valley and its outlying areas
Mon-Khmer (Indigenous)	33	23.7	Modern-day Laos territory
Hmong-Mien (Indigenous)	2	9.7	Northern Laos
Sino-Tibetan (Indigenous)	7	2.9	Uplands of Laos

Source: Open Development Laos, Ethnic minorities and Indigenous Peoples

## 1.2 Legal framework on the rights of Indigenous Peoples

### Map of Distribution by ethno-linguistic families



Source: <http://www.laoatlas.net/Welcome.html>

Although Laos voted in favor of adopting the UN Declaration on the Rights of Indigenous Peoples (UNDRIP) at the United Nations (UN) General Assembly in 2007, the government does not recognize existence of Indigenous Peoples in the country. Rather, it claims that Laos is a multi-ethnic country and all ethnic groups are the same.<sup>109</sup> The Constitution of 2015 states that “the State pursues the policy of promoting unity and equality among all ethnic groups” and forbids actions of division and discrimination.<sup>110</sup>

The legal framework restricts the right of IPs to customary land. Stipulated in Article 17 of the 2015 Lao PDR Constitution and the 2003 Land Law, all lands in Lao PDR are the property of Lao population as a whole.<sup>111</sup>

<sup>109</sup> AIPP, IWGIA, *Indigenous Peoples in ASEAN: Lao PDR*, 2015, available at: [https://aippnet.org/wp-content/uploads/2020/02/15.-Asean-study\\_Laos\\_15\\_July\\_2015\\_Final\\_PM.pdf](https://aippnet.org/wp-content/uploads/2020/02/15.-Asean-study_Laos_15_July_2015_Final_PM.pdf)

<sup>110</sup> UN Committee on the Elimination of Racial Discrimination (CERD). *Reports submitted by States parties under article 9 of the Convention : International Convention on the Elimination of All Forms of Racial Discrimination : 16th to 18th periodic reports of States parties due in 2009 : Lao People's Democratic Republic*, 2011, CERD/C/LAO/16-18, available at: <https://undocs.org/Home/Mobile?FinalSymbol=CERD%2FC%2FLAO%2FCO%2F16-18&Language=E&DeviceType=Desktop>

<sup>111</sup> Manushya Foundation and AIPP, *Lao UPR Factsheet on Indigenous Peoples' Rights*, January 2020, available at: <https://www.manushyafoundation.org/lao-pdr-upr-factsheets>



While the law recognizes permanent and temporary land-use rights for individuals, it fails to define communally held rights of Indigenous communities.<sup>112</sup> With user rights, communities and individuals are entitled to manage and use common land but subject to land grabbing as the government can legally seize the lands where Indigenous communities have been residing for development projects.

Furthermore, the current laws have long violated IPs' socio-economic rights such as the right to an adequate standard of living by empowering the government authorities to relocate IPs. The Law on Resettlement and Vocation enacted in August 2018 allows for "general resettlement" of communities residing in "remote and underdeveloped areas",<sup>113</sup> which expands the government's authority to relocate communities, especially ethnic groups, to suit development projects and business investments. Consequently, IPs often face various difficulties ranging from loss of livelihoods to threats to health, and social isolation. The Decree on Ethnic Affairs, drafted by the Department of Ethnic Affairs and currently under revision, aggravates the abuses of IPs' socio-economic rights. Although it "prescribes the principles, regulations and measures" to "make ethnic groups have unity, equality, respect, and help each other; ensure the participation from all ethnic groups" and "protect their legitimate rights and benefit", the Decree neither addresses IPs' rights to their lands, resources and traditional livelihoods nor ensures education in different ethnic languages.<sup>114</sup> Some provisions even allow the authority to forcefully evict IPs that "live in the hardship and undeveloped areas, risky livelihoods areas, development project-affected areas, and special areas to areas that can be developed and create appropriate permanent jobs and employment".<sup>115</sup> Under the existing legal and institutional framework, IPs continue to experience challenges in accessing education and social services as well as engaging in decision-making processes due to poor infrastructure, far distances, language barriers, and lack of respect for their rights.<sup>116</sup>

### 1.3 The situation of Indigenous Environmental Human Rights Defenders (IEHRDs)

Due to the lack of legal recognition of Indigenous rights and the government's efforts to push for development projects, a large number of ethnic minority groups are increasingly caught up in land disputes and forced to relocate.<sup>117</sup> Tensions between Indigenous rights activists and the authorities have escalated. In a repressive country with a bad human rights record, IEHRDs thus encounter a series of challenges for carrying out their work and are often at risk of arbitrary detention, enforced disappearance, harassment and prosecution.

112 IWGIA, *Indigenous World 2020: Laos*, 11 May 2020, available at: <https://www.iwgia.org/en/laos/3604-iw-2020-laos.html>

113 National Assembly, *Law on Resettlement and Vocation*, 2018, available at: <https://data.laos.opendevlopmentmekong.net/en/dataset/710aeca7-282b-4423-a5cd-fb166a3d9ef2>

114 IWGIA, *Indigenous World 2020: Laos*, 11 May 2020, available at: <https://www.iwgia.org/en/laos/3604-iw-2020-laos.html>

115 IWGIA, *Indigenous World 2020: Laos*, 11 May 2020, available at: <https://www.iwgia.org/en/laos/3604-iw-2020-laos.html>

116 Manushya Foundation and AIPP, *Lao People's Democratic Republic Joint Submission to the UN Universal Periodic Review 35th Session of the UPR Working Group*, 21 July 2019, available at: <https://www.manushyafoundation.org/joint-upr-subm-to-laos-mf-aipp>

117 Freedom House, *Freedom in the World*, Laos, 2019, available at: <https://freedomhouse.org/country/laos/freedom-world/2020>

The government severely restricts freedom of expression, and freedom of assembly and association. The State owns most media outlets, which only reflect government policies. Privately owned publications undergo strict censorship and may face penalties for dissident political commentary. Individuals and activists generally exercise self-censorship for the fear of reprisals, particularly after the disappearance of the prominent civil society leader Sombath Somphone in December 2012.<sup>118</sup> Protests are rare and participation in unsanctioned rallies can lead to lengthy prison sentences.<sup>119</sup> Associations and individual members are disciplined on arbitrary grounds while their funds are subject to monitoring and regulations. Redressing human rights violations is ineffective for IEHRDs and IPs in Laos because of the lack of independent judicial system, long procedural delays, the presumption of guilt, biases, corruption, and the inability to access statutory systems.<sup>120</sup> As a result of the strict controls, many Lao people lack access to information and remedies.<sup>121</sup>

While the digital technologies have opened new space for IEHRDs, who tend to communicate, campaign and advocate online, the government has expanded its control over online speech. In addition to the criminalization of the spread of “fake news” and posts criticizing the government through a series of cyber-security laws, the authority has required individuals and news outlets to register on social media sites with their full names since July 2019.<sup>122</sup> The COVID-19 pandemic along with lockdown measures such as the prohibition of public gatherings and closure of borders has further stifled free expression. Amid the pandemic, those disseminating a video of a land grab were detained and online users were arrested for “spreading rumours aimed at causing public panic” related to COVID-19.<sup>123</sup> With the shrinking online space, IEHRDs have become increasingly vulnerable.

- 
- 118 Human Rights Council, Working Group on Arbitrary Detention, *Opinion No. 61/2017 concerning Lodkham Thammavong, Somphone Phimmasone and Soukan Chaitbad (Lao People's Democratic Republic)*, 15 September 2017, available at: [https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A\\_HRC\\_WGAD\\_2017\\_61.pdf](https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_61.pdf)
- 119 Freedom House, *Freedom in the World*, Laos, 2019, available at: <https://freedomhouse.org/country/laos/freedom-world/2020>
- 120 Manushya Foundation, *Submission to the UN Special Rapporteur on Extreme Poverty and Human Rights on the situation in Lao PDR, for his official country visit from 18 to 28 March 2019*, March 2019, available at: <https://www.manushyafoundation.org/unsr-extreme-poverty-hr-laopdr>
- 121 Manushya Foundation and AIPP, *Lao UPR Factsheet on Civic Space*, January 2020, available at: <https://www.manushyafoundation.org/lao-pdr-upr-factsheets>
- 122 U.S. State Department, *2019 Country Reports on Human Rights Practices: Laos*, 2019, available at: <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/laos/>
- 123 CIVICUS, *Clampdown on expression online persists as Laos slips further down the press freedom rankings*, 29 May 2020, available at: <https://monitor.civicus.org/updates/2020/05/29/clampdown-expression-online-persists-laos-slips-further-down-press-freedom-rankings/>



## 2. Methodology

The methodologies used for this report include desk research, interviews and consultations with IEHRDs at local and national levels. Primary sources including voices, concerns, cases and experiences of IEHRDs were collected directly from Asia Indigenous Peoples Pact (AIPP) and Manushya Foundation's activities. For example, AIPP organized a regional exchange and training on digital security from 30 September to 2 October 2020, where Indigenous human rights activists from ten countries participated and shared their experiences with online interferences, including threats, prosecution, hacking and internet shutdown, in relation to their works on Indigenous rights. AIPP carried out analysis of current challenges while Manushya Foundation supported AIPP to assess legal framework and propose recommendations for IEHRDs, and also engaged with local Indigenous communities to gain insights and identify human rights violations.

This report is also based on desk research, including a systematic literature review of relevant laws and government regulations; reports and observations/recommendations of United Nations (UN) human rights bodies and NGOs; online news articles, expert papers and other publications. It aims to present an analysis of the legal framework on cybersecurity laws and potential impacts on IEHRDs.



Hmong Indigenous Women in traditional dress,  
Vientiane, Lao PDR

### 3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age

**HUMAN DEVELOPMENT INDEX (HDI):** 0.613 (2019)

**NUMBER OF INTERNET USERS IN LAO PDR:** 3.55 million (as of January 2021)

**LEVEL OF FREEDOM:** 13/100 (with 0 being least free and 100 being most free, Freedom in the World 2021 – Freedom House)

**LEVEL OF PRESS FREEDOM:** Ranked 172<sup>nd</sup> out of 180 countries (with 1<sup>st</sup> being highest level of press freedom, World Press Freedom Index 2021 - Reporters Without Borders)

**LEVEL OF FREEDOM ON THE NET:** N/A

**GLOBAL CYBERSECURITY COMMITMENT:** Ranked 131<sup>st</sup> out of 182 countries with a score of 20.34/100 (with 1<sup>st</sup> being highest and 182<sup>nd</sup> being the lowest commitment – ITU Global Cyber Security Index)

The fundamental rights of Lao citizens are provided in Constitution whereas the legislative framework and policies excessively restrict the rights to information, freedom of expression, association and assembly. With vaguely worded and restrictive provisions, relevant laws exercise a chilling effect on IPs and IEHRDs. Increasingly aware of the restrictions imposed on offline activities, Laotians are turning to internet and social media to express their concerns and seek uncensored information. In January 2020, there were 3.1 million internet

users in Laos - an increase of 188,000 (6.5%) between 2019 and 2020. The number of social media users in Laos also grew by 328,000 (12%) between April 2019 and January 2020.<sup>124</sup> However, the government extended its control by regulating internet communication through a series of cybersecurity laws. Legal provisions and policies restricting and criminalizing online expression continue to be invoked to detain individuals peacefully exercising their rights.

#### 3.1 Constitutional provisions and laws stipulating the rights of IEHRDs

The Lao PDR Constitution acknowledges a series of rights. Article 34 of the Constitution provides for the fundamental rights of Lao citizens as “the State acknowledge, respect, protect, and guarantee the human rights including fundamental rights of the citizen in accordance with the law.” Article 35 guarantees equality before the law that “Lao citizens are all equal before the law irrespective of their gender, social status, education, beliefs and ethnic group.” The rights to freedom of speech and press; assembly and associations are recognized under Article 44 of the Constitution, but those rights should “not (be) contrary to the laws”. Article 41 of the Lao Constitution allows people to file complaints and petitions to the National Steering Committee on Human Rights, under the National Legislative Assembly.<sup>125</sup>

<sup>124</sup> DataReportal, *DIGITAL 2020: LAOS*, 18 February 2020, available at: <https://datareportal.com/reports/digital-2020-laos>

<sup>125</sup> Amended Constitution of the Lao PDR, (2015) available at: [https://www.parliament.go.th/ewtadmin/ewt/ac/ewt\\_dl\\_link.php?nid=119&filename=parsystem2](https://www.parliament.go.th/ewtadmin/ewt/ac/ewt_dl_link.php?nid=119&filename=parsystem2)

Further, the 2019 Decree on Environmental Impact Assessments, No. 21/PMO, provides for protective laws and policies in the context of development projects and business investment affecting IPs. Article 56 stipulates rights of Project Affected Peoples, including the right to receive and access to information; be fairly compensated and resettled; be supported on health care; be supported through the promotion of culture, religion and belief conservation, and gender equality; participate in the consultation. Particularly, those affected can “submit recommendations to project owner or complaints to concerned government organizations on the improper and unfair mitigation of environmental impact generated by the investment projects and activities”, which allows IPs and IEHRDs to voice their concerns over the development projects and pursue an administrative remedy. It also provides obligations of Project Owner, including the responsibility to consider and implement the project affected people requests in Article 59, as well as provisions for dispute settlement.<sup>126</sup>

Nevertheless, these protective laws are poorly enforced and implemented on the ground. With other restrictive laws, IPs and IEHRDs are often deterred from exercising their rights, resulting in marginalization and exclusion.

## 3.2 Legal framework restricting offline activities of HRD

### 3.2.1 Penal Code<sup>127</sup>

#### (A) Provisions Curbing Freedom of Expression

Legal provisions in Penal Code 2017 that curb freedom of expression contain vague and broadly formulated offenses. These include provisions on “propaganda against the state” (Article 117) and criminal defamation, libel and insult (Articles 205 and 206).

Article 117 criminalizes “any individual who uses propaganda to slander the Lao PDR, or who use false news to spread disorder through oral communications, writings, publications, newspapers, films, videos, photographs, documents or other means against the State will be punished by one to five years of imprisonment and shall be fined from 500,000 Kip to 20,000,000 Kip”. Articles 205 and 206 stipulate that any person who defames and libels in causing severe damage to the dignity of other persons through oral, written or other means shall be punished by three months to one year of imprisonment or by re-education without deprivation of liberty and shall be fined according to the law.

#### (B) Provisions Restricting Freedom of Assembly and Association

Articles 110 and 124 of the Penal Code are often used to restrict freedom of assembly or association and criminalize actions of human rights defenders and journalists on grounds of social disorder, social damage and national security. Article 110 states that “Lao citizens who, in relation or in cooperation with foreigners or foreign organizations, lead activities to undermine the independence, sovereignty, territorial integrity or basic political, defense, security, economic or sociocultural interests of the Lao PDR will be punished by the deprivation of liberty from 10 to 20 years and will

<sup>126</sup> Decree on Environmental Impact Assessments, No. 21/PMO (2019), available at: [https://laoofficialgazette.gov.la/kcfinder/upload/files/EIA%20Decree\\_English\\_unofficial%20%20translation%2011.6.2019.pdf](https://laoofficialgazette.gov.la/kcfinder/upload/files/EIA%20Decree_English_unofficial%20%20translation%2011.6.2019.pdf)

<sup>127</sup> Decree of the President on the Promulgation of the Amended Penal Law No. 142/PO, (9 November 2005), available at: <http://un-act.org/publication/view/lao-pdrs-penal-law-2005/>

be fined from 10,000,000 Kip to 500,000,000 Kip or shall be punished by a seizure of properties and confined to home custody or sentenced to life imprisonment or the death penalty". According to Article 124, "any individual who organizes or participates in a group organization for the purpose of demonstrations, protest marches or other, in view of causing turmoil likely to generate social damage, will be punished by one to five years of imprisonment and shall be fined from 200,000 Kip to 50,000,000 Kip".

Under the provisions of the Penal Code, Lao authorities continue to arbitrarily arrest and detain government critics and charge IPs and IEHRDs protesting against land grabs. A case in point is the arrest of 15 residents of Yeub village in Thateng district of Sekong Province by the police in 2017 for protesting by cutting down rubber trees planted on their land by a Vietnamese rubber company, after their land was granted by the government to the Lao-Vietnam Friendship Rubber Company. Most of them are from the Katou ethnic minority.<sup>128</sup>

### 3.2.2 Decree on Associations

Enacted in November 2009, Decree No.115 on Associations provides for the registration of non-profit civil society organizations (CSOs), including economic, social welfare, professional, technical, and creative associations, at the district, provincial, or national level. But the registration process is extremely cumbersome and slow.<sup>129</sup> The Decree No. 238 on Associations that came into effect in November 2017 further tightens controls and restrictions on CSOs. The formation of CSOs can be unreasonably controlled and prohibited by the government while their activities and finances have to go through strict inspection and monitoring. The government has the power to order the dissolution of associations on arbitrary grounds and without their right to appeal, and discipline associations and individual members on arbitrary grounds. The Decree also includes provisions on the criminalization of unregistered associations and prosecution of their members.<sup>130</sup>

In summary, the Decree on Associations contains considerable and onerous regulations and prohibitions on associations, giving unrestrained power to government officials to arbitrarily forbid activities undertaken by CSOs, which are deemed to threaten national security and social orders. As a result, IPs and IEHRDs who wish to set up associations to defend their rights are discouraged due to the restrictions and barred from carrying out any human rights related activities.

128 RFA, Two Lao Protest Villagers Seriously Ill in Jail, 1 February 2019, available at: <https://www.rfa.org/english/news/laos/villagers-02012019162329.html> ; Manushya Foundation, Submission to the UN Special Rapporteur on Extreme Poverty and Human Rights on the Situation in Lao People's Democratic Republic (PDR), (March 2019), available at: <https://www.manushyafoundation.org/unsr-extreme-poverty-hr-laopdr>

129 FIDH, Lao Movement for Human Rights (LMHR), *Joint submission for the adoption of the List of Issues*, Lao PRD, available at: <https://www.refworld.org/pdffd/5979fa624.pdf>

130 Decree No. 238 on Associations (2017), available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjzru3Mg7vtAhUTa94KHSyVAFUQFjADegQIARAC&url=http%3A%2F%2Ffloacs-kis.org%2Fwp-content%2Fuploads%2F2017%2F11%2FEnglish-translation-of-Decree-238-on-Association-002.docx&usg=AOvVaw3kbHXtmA-MP4jzfZJsgH5O>

### 3.2.3 Media Act and Decree No. 377 on Management of Foreign Media

The State control over the media with the 2016 amendments to the Media Act of 2008 and the Decree No. 377 on Management of Foreign Media of November 2015, which impose restrictions to ensure strict adherence to and promotion of government policy.

Under Article 39 of the amended Media Act, the formation of a media organization needs to fulfill five criteria defining the media organization, media type, ideology, objectives, organizational structure, office, and necessary vehicles and equipment.<sup>131</sup> The Decree No. 377 on Management of Foreign Media, which came into force in January 2016, contains provisions on prior censorship, the requirement on registration and prior approval, as well as obligations of foreign media to abide by the traditions and culture of the Lao PDR. For example, foreign media agencies and journalists, diplomatic missions and international organizations must submit their work to the Ministry of Foreign Affairs for consideration and approval prior to publication under Articles 14 and 18 of the Decree. They are also required to abide by the traditions and culture of Lao under its Article 19. Moreover, the appointment of the head of the office of a foreign media agency as well as other staff of these agencies must undergo approval by the Ministry of Foreign Affairs under Article 11.<sup>132</sup>

The Media Act and the Decree allow the authorities to have broad discretion to control information and communication, which greatly undermines the independence of both national and international media. The definition and interpretation of “the traditions and culture of Lao PDR” lack sufficient clarity and precision, leading to undue interference and overly broad discretion from the authorities to restrict the exercise of the right to freedom of expression. Consequently, IPs and IEHRDs are hindered from advocating through media and accessing accurate and uncensored information.

## 3.3 Cyber-security laws and policies restricting online activities of IEHRDs

### 3.3.1 Decree No. 327 on Internet-Based Information Control/Management<sup>133</sup>

On 16 September 2014, the Lao government approved Decree No. 327 on Internet-Based Information Control/Management, which entered into force on 1 October 2014. The Decree contains a number of provisions that appear to unduly restrict the right to freedom of expression and opinion and criminalize online criticism and the circulation of “false information online”.

131 Inquirer Net, *Laos orders registration of social media news platforms*, 16 July 2019, available at: <https://technology.inquirer.net/89044/laos-orders-registration-of-social-media-news-platforms>

132 OHCHR, *Joint Letter from Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the situation of human rights defenders to Lao PDR*, LAO 2/2016, 6 May 2016, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=19899>

133 Decree on Information Management on the Internet (2014), available at: [http://www.laoservicesportal.com/images/download/Announcement\\_2017040223045832.pdf](http://www.laoservicesportal.com/images/download/Announcement_2017040223045832.pdf)

### Under Article 10, content not allowed for dissemination on the internet includes

- “false or misleading information against the Lao People’s Revolutionary Party or the Government”;
- “false propaganda” with the aim of undermining social unity and the solidarity among ethnic/minority groups and nations;
- “edited photos and other photos that the law of the Lao PDR has prohibited, including photos discrediting the Lao tradition”; and
- national secrets, military secrets or “other secrets” as indicated in Lao PDR’s legislation and regulation.

These provisions are extremely vague in relation to their interpretation and concrete application. Terms such as “false”, “misleading” or “untrue” information are not clarified. Article 16 provides for the responsibilities of internet users, which prohibits not only the dissemination of information listed in Article 10 but also commenting in support of restricted content. Furthermore, Article 8 requires internet users to indicate their names, surnames and current addresses when creating their profiles on social media.

In addition to regulating individuals for the information or comment that they post or disseminate online, the Decree also stipulates that web managers and Internet Service Providers (ISPs) can also be held responsible for failing to ensure that content and information prohibited in Article 10 are not circulated and disseminated. For example, Article 15 prohibits ISPs from facilitating the circulation of information or ideas “attacking or destroying government-party policy”, as well as information that may “impact national defense and peaceful activities”. Again, the provisions that hold web managers and ISPs responsible for behavior “in any manner that violates the regulations and laws” are vaguely worded.

Article 26 lists a number of sanctions to punish individuals, legal entities or organizations that violate the Decree ranging from warnings to education, penalty, fines and criminal prosecution depending on the severity of the case. Nevertheless, it fails to determine the behavior to which the sanction corresponds, allowing the authorities to arbitrarily punish criticism against the government policies, including land grabbing.

### 3.3.2 Law on Prevention and Combating Cyber Crime<sup>134</sup>

The Law on Prevention and Combating Cyber Crime (2015) reinforces the government authority to criminalize web content based on vague grounds. The law prohibits certain content on the internet, including deceptive statements and statements against the government and Lao PDR. According to Article 8, “causing damages via online social media” is identified as one of the cybercrimes. In particular, Article 13 provides that actions “causing damages via online social media” include applying “false, misleading and deceptive information” and bringing information that damages “national security, peace, order in society, national culture and fine tradition of the nation” into computer system. Such actions can be punished by imprisonment from three months to three years and fine from 4,000,000 Kip to 20,000,000 Kip according to Article 62. Article 39 also provides for general prohibitions, including propagating to destroy or oppose against the political regime in order to cause turbulence in

134 Law on Prevention and Combating Cyber Crimes No. 61/NA, (15 July 2015), available at: [https://www.laocert.gov.la/ftp\\_upload/Cyber\\_Crime\\_Law\\_EnVersion.pdf](https://www.laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf)



society. Service providers can be punished for “providing conditions or facilities for activities of cybercrime” under Article 40.

The law also provides for the Sector of Posts and Telecommunications – an organization to monitor, track, advise and prevent emergency incidents and collect statistics under Articles 29 and 30. However, restrictions on the collection, use and disclosure of data and statistics by the authorities are not provided in this law. Overall, this law raises concerns over government’s unrestricted authority to silence criticisms considered as “false” information and against “national security, peace, social order and fine tradition of the nation”. Such terms remain open to interpretation.

### 3.3.3 Penal Code 2017

Article 117 of the Penal Code 2017 (Article 65 of its predecessor Penal Code 2005) extends the range of prohibitions applied to online space by criminalizing “propaganda against the government” and prosecuting activists, who question the government’s policies on social media. It provides for penalizing anyone, who conducts “propaganda activities against and slandering the Lao PDR, [...] or circulating false rumours causing disorder by words, in writing, through print, newspapers, motion pictures, videos, photographs, documents or other media which are detrimental to the Lao PDR or are for the purpose of undermining or weakening State authority”, with prison terms of one to five years and a fine of five to 20 million Kip (approximately US\$570 to US\$2,280).<sup>135</sup>

Yet, the prohibition based on “propaganda against Lao PDR” appears to contradict the requirements prescribed by Article 19 (3) of the International Covenant on Civil and Political Rights (ICCPR), which states that certain restrictions on freedom of expression must be determined by law as necessary for respect of the rights or reputations of others or for the protection of national security or of public order, health or morals.<sup>136</sup> The Human Rights Committee, in its General Comment, has noted that the restrictions “must conform to the strict tests of necessity and proportionality” and that it is not compatible to invoke the laws relating to national security “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 information”.<sup>137</sup>

### 3.3.4 Agencies and policies

The Ministry of Post, Telecommunication and Communication is responsible for online surveillance, tracking, and monitoring of political criticism or comments against the Party and government leadership. Provided by the Law on Prevention and Combating Cyber Crimes, it has authority to direct ISPs to terminate internet services of users found violating the law and claim and report on cybercrime offenses to the Public Prosecutor.<sup>138</sup> The National

135 FIDH, *Woman detained for criticizing the government online*, 16 September 2019, available at: <https://www.fidh.org/en/region/asia/laos/woman-detained-for-criticizing-the-government-online>

136 International Covenant on Civil and Political Rights (1976), available at: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

137 Human Rights Committee, *General comment No. 34 – Article 19: Freedoms of opinion and expression*, 12 September 2011, available at: <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf> <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25397>

138 Law on Prevention and Combating Cyber Crimes No. 61/NA, (15 July 2015), available at: [https://www.laocert.gov.la/ftp\\_upload/Cyber\\_Crime\\_Law\\_EnVersion.pdf](https://www.laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf)



Internet Committee under the Prime Minister's Office administers the internet system that requires ISPs to submit quarterly reports and link their gateways to facilitate monitoring.<sup>139</sup>

The Ministry of Information, Culture and Tourism takes a key role in controlling media including TV, radio and printed publications. In January 2012, it ordered cancellation of the popular radio program "Talk of the News" as the show encouraged political and social debate on a variety of topics, including land grabs and corruption. Yet, the authority gave no explanation for the cancellation.<sup>140</sup> In recent years, the Ministry is also responsible for approving and controlling the content of information and data exchanged on the internet. In July 2019, it issued an announcement demanding administrators register their accounts with the Ministry's Media Department. Online media outlets and any individual who set up a social media account that provides information for distribution to the public must register.<sup>141</sup>



People in Vang Vieng were returning home after a hard day's work on the field.

139 U.S. State Department, *2019 Country Reports on Human Rights Practices: Laos*, 2019, available at: <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/laos/>

140 Human Rights Watch, *Human Rights Watch Concerns on Laos*, 5 November 2015, available at: <https://www.hrw.org/news/2015/11/05/human-rights-watch-concerns-laos>

141 Inquirer Net, *Laos orders registration of social media news platforms*, 16 July 2019, available at: <https://technology.inquirer.net/89044/laos-orders-registration-of-social-media-news-platforms>

## 4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases

### 4.1 Arrest and prosecution of IEHRDs for online criticism

With broad definition and vaguely worded offenses, cybersecurity laws and policies in Laos criminalize online speech in the name of protecting national security and social order and combating “false information” in contravention international laws. The right to freedom of expression is violated by the misuse of such provisions to control the critics arbitrarily and arrest even prosecute IPs and IEHRDs voicing concerns in the face of land concessions. Activists who are charged under these laws can be sentenced to at least three years in prison without fair trials. As a result, the ability of IEHRDs to advocate online and seek justice has been diminished.

#### **Case of Muay who was charged under Article 117 for online advocacy<sup>142</sup>**

In November 2019, Houayheuung Xayabouly also known as Muay, from Champasak Province, was sentenced to 5 years in prison and a 20 million Kip fine under Article 117 of the Penal Code on charges of conducting propaganda activities against Lao PDR. She is an environmental activist and woman human rights defender, who repeatedly used Facebook to criticize the Lao government. Her first online advocacy activity was on 1 October 2017 when she recorded a video highlighting the financial burden that she and other local villagers face for paying a heavy fee for crossing a local toll bridge. After the video went viral, she was visited by local police officers, who warned her against criticizing the government. Since May 2018, she had been raising awareness about government corruption. Later, she was dismissed from her job at the tour guide company where the employer gave no reason but was receiving pressure to do so. After the 2018 collapse of the auxiliary dam at the Xe-Pian Xe-Namnoy hydropower project, she collected money, food and clothes for the displaced families and continued posting videos on Facebook to criticize the mishandling of the dam collapse. In September 2019, she posted another video criticizing the government’s slow response in providing relief to the affected people and calling for solutions to prevent similar incidents from happening in the future. Shortly after, she was arrested without a warrant. Her request for a lawyer was denied but one was assigned just before the trial, who allegedly never discussed the details of the case with her. She is currently in her prison serving her sentence.

142 OHCHR, *Joint Letter from Special Rapporteur on the situation of human rights defenders; Working Group on Arbitrary Detention; Working Group on the issue of human rights and transnational corporations and other business enterprises; Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on extreme poverty and human rights; Special Rapporteur on violence against women, its causes and consequences and Working Group on discrimination against women and girls to Lao PDR*, 13 July 2020, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25397>

### Case of a pro-democracy activist imprisoned for Facebook posts<sup>143</sup>

In June 2015, the pro-democracy activist Bounthanh Thammavong was arrested for “disseminating propaganda against the state” on Facebook after he criticized the government’s policies and actions. The Vientiane Supreme Court sentenced him to four years in jail. Prior to his arrest, Bounthanh had been forced into exile from Laos and subsequently became a citizen of Poland where he founded the Organization of Lao Students for Independence and Democracy. In 2010, he returned to Laos to run a business with assurances from Lao officials that he would not face arrest on his return. He was the first in Laos who was arrested and sentenced to jail for online speech after Decree No. 327 on Internet-Based Information Control/Management went into effect in October 2014. On 21st June 2019, he was released from prison after serving four-year term and returned to Poland.

### Case of three activists criticizing the government online<sup>144</sup>

In March 2017, three activists, Lodkham Thammavong, Soukane Chaithad and Somphone Phimmason were convicted for publishing posts on Facebook in which they criticized the government in relation to corruption, deforestation and human rights violations, apart from taking part in a demonstration outside the Lao Embassy in Thailand to express concerns over the government’s human rights record. The three individuals had been charged under Article 56 (acts of betrayal towards the nation, now as Article 110 of the 2017 Penal Code), Article 65 (propaganda against Lao, now as Article 117 of the 2017 Penal Code) and Article 72 (group gathering for turmoil generating purposes, now as Article 124 of the Penal Code). Ms. Lodkham was sentenced to 12 years’ imprisonment while Mr. Somphone was sentenced to 20 years’ imprisonment and Mr. Soukan was sentenced to 16 years’ imprisonment. Their cases appeared to be in retaliation for their peaceful and legitimate human rights work and exercise of their rights to freedom of expression and freedom of peaceful assembly. In 2017, UN Working Group on Arbitrary Detention declared their detention to be arbitrary.

## 4.2 Poor access to information for IEHRDs and IPs

As cybersecurity laws prohibit the spread of “false information” without a clear definition of what constitutes “false” or “untrue” information, such vague provisions are invoked not only to target any dissenting voice and silence any form of criticism but also to block uncensored information on the policies and practices of the ruling Party or the government. Strict online information controls further lead to poor access to information and lack of oversight on massive development projects, which hinders the activities of IEHRDs and affects the lives of people.

### Case of lack of information in 2018 Xe Pien-Xe Nam Noy dam collapse

In July 2018, the Xe Pien-Xe Nam Noy hydropower dam collapse resulted approximately 7,000 people displaced by the floods and 43 people reported dead and 28 missing.<sup>145</sup> In the absence of meaningful consultations of the hydropower project and immediate notification

143 RFA, *Lao-Polish Political Prisoner Released From Jail After Serving Four-Year Term*, 21 June 2019, available at: <https://www.rfa.org/english/news/laos/lao-polish-political-prisoner-released-06212019120951.html>

144 Human Rights Council, Working Group on Arbitrary Detention, *Opinion No. 61/2017 concerning Lodkham Thammavong, Somphone Phimmason and Soukan Chaithad (Lao People’s Democratic Republic)*, 15 September 2017, available at: [https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A\\_HRC\\_WGAD\\_2017\\_61.pdf](https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_61.pdf)

145 OHCHR, *Joint Letter from Working Group on business, Special Rapporteur on environment, Special Rapporteur on housing, Special Rapporteur on indigenous peoples, Special Rapporteur on internally displaced persons, Special Rapporteur on poverty, Special Rapporteur on water and sanitation to Lao PDR*, 17 April 2020, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25088>

from the authority of the dam collapse, many villagers were unaware of the situation and even had no knowledge of the existence of the dam. After the dam collapse, people shared lots of first-hand information on social media to help affected people and some activists such as Houayheuag Xayabouly “Muay” questioned the government’s inaction. However, the government continued to stifle online information and dissents and keep the truth from the public. The Prime Minister issued a warning letter to all Lao citizens requesting them not to believe the misinformation of the foreign media and social media and instead to only trust information shared by state-owned media.<sup>146</sup> Meanwhile, a National Investigation Committee was established and later submitted a report on analysis of the causes to the Lao government - the findings of which were never released in full to the public.<sup>147</sup> The relevant business enterprises have not fulfilled their obligations to ensure that the businesses respect human rights. They neither organized meaningful consultations with the villagers from the early stage of the project nor developed and implemented a warning system with response plans agreed upon by the affected communities.<sup>148</sup> It was also reported that companies building the dam even knew that it was deteriorating prior to the collapse but failed to notify the authority earlier.<sup>149</sup>

### 4.3 User privacy at risk

Although the Lao government’s technical ability to monitor internet usage is limited and the authorities do not block access to websites,<sup>150</sup> the existing cybersecurity laws and policies largely impose a risk of surveillance and privacy breach. Under the guise of national security, the cybersecurity laws grant the government sweeping powers to monitor the use of the internet and the content shared and to collect relevant data when there is a perceived security threat. The government controls domestic internet servers and maintains infrastructure to route all internet traffic through a single gateway, thereby allowing it to monitor and restrict content.<sup>151</sup> Moreover, the authorities can inform ISPs and data storage persons to provide users’ information without a prior request and obtaining a warrant from the court,<sup>152</sup> which curtails the right to privacy. Requiring individuals to register on social media sites with their full names and addresses also limits the freedom to use those media anonymously.<sup>153</sup> This could allow for the misuse of this power to collect information, which could subsequently be wrongly used to charge IEHRDs for other crimes such as defamation

146 Manushya Foundation and AIPP, *Lao UPR Factsheet on Civic Space*, January 2020, available at: <https://www.manushyafoundation.org/lao-pdr-upr-factsheets>

147 OHCHR, *Joint Letter from Working Group on business, Special Rapporteur on environment, Special Rapporteur on housing, Special Rapporteur on indigenous peoples, Special Rapporteur on internally displaced persons, Special Rapporteur on poverty, Special Rapporteur on water and sanitation to Lao PDR*, 17 April 2020, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25088>

148 OHCHR, *Joint Letter from Working Group on business, Special Rapporteur on environment, Special Rapporteur on housing, Special Rapporteur on indigenous peoples, Special Rapporteur on internally displaced persons, Special Rapporteur on poverty, Special Rapporteur on water and sanitation to Lao PDR*, 17 April 2020, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25088>

149 New York Times, *A Day Before Laos Dam Failed, Builders Saw Trouble*, 26 July 2018, available at: <https://www.nytimes.com/2018/07/26/world/asia/laos-dam-collapse.html>

150 U.S. State Department, *2019 Country Reports on Human Rights Practices: Laos*, 2019, available at: <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/laos/>

151 U.S. State Department, *2019 Country Reports on Human Rights Practices: Laos*, 2019, available at: <https://www.state.gov/reports/2019-country-reports-on-human-rights-practices/laos/>

152 Law on Prevention and Combating Cyber Crimes No. 61/NA, (15 July 2015), available at: [https://www.laoert.gov.la/ftp\\_upload/Cyber\\_Crime\\_Law\\_EnVersion.pdf](https://www.laoert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf)

153 Decree on Information Management on the Internet (2014), available at: [http://www.laoservicesportal.com/images/download/Announcement\\_2017040223045832.pdf](http://www.laoservicesportal.com/images/download/Announcement_2017040223045832.pdf)

and propaganda against Lao PDR to suit the needs of the authorities. Further, as there is no specific law on personal data protection in Laos,<sup>154</sup> IEHRDs who advocate online can be vulnerable to data breaches caused by third parties.

## 4.4 Limited access to remedy: Compensation and Grievance mechanisms

Access to remedy in the form of appeal against the abuse of power by public authorities is not specifically provided in relevant cybersecurity laws. That exacerbates the pre-existing vulnerabilities of IEHRDs and IPs to human rights violations. Although people have the right to file complaints and petitions under the Constitution, they have few avenues for redress, especially with the weak civil society sector that is prevented from advocating on behalf of those affected.

In the context of development projects and investments, IPs are denied effective remedies with poor resettlement conditions and delayed compensation.<sup>155</sup> As in the case of the Lao-China railway project, around 500 families affected by the construction in Oudomxay province still lack adequate shelter and access to clean water while many families have yet to see any compensation even though the project is now more than 90 percent complete.<sup>156</sup> Due to the political sensitivity surrounding such projects and investments, IPs are inhibited from accessing company mechanisms for redress for fear of reprisal.<sup>157</sup>

IPs and IEHRDs who petition against development projects or detention of activists are often subjected to unjust suppression ranging from disregard to threats, arrests, detention and ill-treatment. For example, in June 2020, ten families representing Xiengda villagers, who have refused offers of compensation for their land, went to the capital to petition the Lao Prime Minister for help but were turned away by authorities and told to go home and stop making trouble.<sup>158</sup> In another case of three activists charged for online speech, their families had no access to redress. Family of one of the activists, Mr. Soukan, lodged a complaint regarding his detention at the local police station but there was no further response from the authority. Another activist, Mr. Somphone's family was warned by the authority that they would face legal action and be charged with committing crimes against national security if they tried to find the whereabouts of these activists.<sup>159</sup> Thus, victims of human rights abuses and their families routinely avoid seeking justice for fear of reprisals.

154 ZICO Law, *Personal Data Protection in ASEAN*, April 2019, available at: [https://zico.group/wp-content/uploads/resources/asean\\_insiders/ASEAN\\_Insiders-PDPA.pdf](https://zico.group/wp-content/uploads/resources/asean_insiders/ASEAN_Insiders-PDPA.pdf)

155 Manushya Foundation and AIPP, *Lao UPR Factsheet on Indigenous Peoples' Rights*, January 2020, available at: <https://www.manushyafoundation.org/lao-pdr-upr-factsheets>

156 RFA, *Thousands Wait for Railway Compensation in Laos' Oudomxay Province*, 16 November 2020, available at: <https://www.rfa.org/english/news/laos/railway-11162020150345.html>

157 ABC News, *Dam collapse highlights risks to communities as Laos seeks to become hydroelectricity hub*, 3 August 2018, available at: <https://www.abc.net.au/news/2018-08-03/dam-collapse-highlights-risks-to-communities-in-laos/10071836>

158 RFA, *Lao Villager Held in Detention Three Months After Land Protest in Vientiane*, 15 June 2020, available at: <https://www.rfa.org/english/news/laos/held-06152020155938.html>

159 Human Rights Council, Working Group on Arbitrary Detention, *Opinion No. 61/2017 concerning Lodkham Thammavong, Somphone Phimmason and Soukan Chaitthad (Lao People's Democratic Republic)*, 15 September 2017, available at: [https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A\\_HRC\\_WGAD\\_2017\\_61.pdf](https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_61.pdf)



## 5. Recommendations

### 5.1 Recommendations to the government

**5.1.1.** Decriminalize online speech and emphasize the internet as a space for exercising freedom of opinion and expression in line with international human rights laws, including Article 19 of the UN Declaration on Human Rights and of the ICCPR.

**5.1.2.** Reform existing laws and policies, including to provide clearer terms and definitions of vague restrictive provisions, so as to ensure that IEHRDs and IPs can fully enjoy their right to free speech without self-censorship or fear of prosecution and in accordance with the Human Rights Committee's Concluding Observations<sup>160</sup>. This includes revising the Media Act, Decree No. 327 on Internet-Based Information Control/Management, the 2015 Law on Prevention and Combating Cyber Crime and provisions of the Criminal Code.

**5.1.3.** Guarantee the entire population unfettered access to information as noted in the Report of the Special Rapporteur on extreme poverty and human rights<sup>161</sup>, including through promotion of independent media, particularly online media, which individuals can rely on, especially in the situation of life risk.

**5.1.4.** Refrain from forcing tech companies as well as ISPs to obey the government censorship and allow them to comply with their responsibilities to respect human rights in line with UN Guiding Principles on Business and Human Rights (UNGPs) and also discontinue requiring netizens to register their personal information so they can operate anonymously.

**5.1.5.** Release all activists detained for exercising their right to freedom of peaceful assembly and freedom of speech, review their cases to prevent further harassment and also provide remedies for victims of arbitrary arrests and enforced disappearances.

**5.1.6.** Begin the process of establishing a human rights institution with a mandate to protect the full range of human rights and in full compliance with the Paris Principles in line with the Human Rights Committee's concluding observation<sup>162</sup> so that such institution can also act as a grievance mechanism.

**5.1.7.** Provide remedies for loss of livelihoods, environmental damage and land degradation taking into account IPs' traditional lifestyles, including fair and adequate compensation.

**5.1.8.** Remove barriers to access effective judicial remedies for IPs through courts, including through provision of language interpretation and free legal aid services, and ensure prompt investigation into complaints filed against development projects, state authorities, law enforcement officials and companies.

**5.1.9.** Require free, prior and informed consent (FPIC) of IPs prior to any project affecting their lands, territories and resources in line with international human rights standards,

<sup>160</sup> Human Rights Committee, *Concluding observations on the initial report of the Lao People's Democratic Republic*, para 33-34, 23 November 2018, available at: [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fLao%2fCO%2f1&Lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fLao%2fCO%2f1&Lang=en)

<sup>161</sup> Human Rights Council, *Visit to the Lao People's Democratic Republic – Report of the Special Rapporteur on extreme poverty and human rights*, para 19, 20 June 2019, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/177/01/PDF/G1917701.pdf?OpenElement>

<sup>162</sup> Human Rights Committee, *Concluding observations on the initial report of the Lao People's Democratic Republic*, para 8, 23 November 2018, available at: [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fLao%2fCO%2f1&Lang=en](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fLao%2fCO%2f1&Lang=en)

including through amendment of the Decree on Environmental Impact Assessments and adoption of necessary new laws and policies.

## 5.2 Recommendations to digital technology companies

**5.2.1** Ensure the companies' terms of service and policies are uniform and comply with international standards on freedom of expression and protection of data privacy, which are reviewed regularly to ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological and societal developments in line with the obligation to respect human rights under the UNGPs.

**5.2.2.** Ensure that any request, order or command to access information is based on a justifiable law, which is subject to external and independent oversight and demonstrates necessary as well as proportionate means to achieve one or more legitimate aims.

**5.2.3.** Publish regular information on their official websites regarding the legal basis of requests made by governments and other third parties as well as the number or percentage of requests complied with, along with the content or accounts restricted or removed under the company's own policies and community guidelines.

**5.2.4.** Provide company-level remedies and grievance redress mechanisms – both physical and virtual – to victims affected by adverse impacts of cybersecurity responses that violate their rights.

**5.2.5.** Collaborate with the government and civil society to develop technology that promotes and strengthens human rights.

## 5.3 Recommendations to project developers and investors

**5.3.1.** Take all necessary and lawful measures to ensure that business practices do not cause, contribute or remain complicit in human rights violations, including the rights of IPs and IEHRDs.

**5.3.2.** Facilitate partnership of businesses with IPs and IEHRDs to assist in the realization of the UNGPs and the Sustainable Development Goals (SDGs).

**5.3.3.** Conduct assessments and due diligence processes to determine the impact of business activities on IPs with respect to individual and community rights with full participation of and consultation with affected IPs and IEHRDs in those assessments and processes.

**5.3.4.** Disclose information related to planned and ongoing large-scale development projects in a timely and accessible manner to the affected communities and IEHRDs.

**5.3.5.** Establish and participate in effective non-State-based grievance mechanisms, including at operational levels.

## 5.4 Recommendations to IEHRDs

**5.4.1.** Engage in the process of understanding digital threats to civic space, identify and document internal and external threats to the freedom of expression with respect to the legal framework.

**5.4.2.** Use encrypted communication in daily works, choose online platforms that allow



users to send encryption-protected information to others and collect and store very little data about users to mitigate surveillance.

**5.4.3.** Ensure that the software versions are up to date and authentication inside and out is upgraded.

**5.4.4.** Increase engagement with business and the government in support of Indigenous rights and digital rights, provide recommendations on the implementation of cybersecurity laws and laws regarding IPs.

**5.4.5.** Hold implementing authorities and officials liable for the misuse of their powers or information obtained while carrying out their duties under cybersecurity laws.





The girl with her traditional house, Luang Namtha, Laos







# MYANMAR

Prepared by Open Development Initiative

# 1. Status of legal recognition of the rights and identities of Indigenous Peoples

Myanmar's ethnic groups are among the world's most marginalized peoples due to socio-political exclusion.<sup>163</sup> Britain's colonization of Myanmar made indigeneity a political issue, and after independence implementation of "Burmanization" by the military junta in 1962<sup>164</sup> further marginalised Indigenous Peoples. The rights of Indigenous Peoples in Myanmar have limited constitutional protection. This is due to the fact that Myanmar's constitutional protections extend only to citizens<sup>165</sup>, and not all ethnic groups are considered citizens. Laws are used more to take away protections from Indigenous Peoples than to protect them. At present, the 1982 Citizenship Law states that all citizens in Myanmar are "Indigenous" or a "national race" (*tain-yin-tha*), but does not permit self-identification as Indigenous, which is contrary to the UN Declaration of the Rights of Indigenous Peoples (UNDRIP) that Myanmar voted in favor of at the UN General Assembly.<sup>166</sup> Indigenous rights activists and communities themselves use the term Indigenous Peoples (*hta-nay tain-yin-tha* (ဣန္ဒြေတိုင်းရင်းသား)) as intended in UNDRIP.<sup>167</sup> In this report, the term "Indigenous Peoples" will be used to refer to people who identify with an ethnic identity and/or being Indigenous to Myanmar.

Myanmar is one of the most diverse countries in Southeast Asia. According to the Myanmar 2014 census, there are officially 135 ethnic groups. Nonetheless, under the 1982 Citizenship Law, only eight ethnic groups (Kachin, Kayin, Shan, Mon, Karenni, Chin, Burman and Arakan) are recognized as national races (*tain yin tha* တိုင်းရင်းသား).<sup>168</sup> This identification was presented in Myanmar before 1823 as "national races", in which the remaining ethnic groups belong to the eight national races.<sup>169</sup> This categorization of national races was adopted from the British census of 1931, based on language.<sup>170</sup> There are some Indigenous minorities (Pa-O, Wa, Kokang, Palaung, Akha, Danu, Naga, Tavoy and Lahu), who do not consider themselves among those eight ethnic groups but are not specifically referenced in the constitution.<sup>171</sup> *Tain-yin-tha* is officially translated as national races (*tain-yin-tha*) by the

163 Myanmar Centre for Responsible Business, Institute of Human Rights and Business and Danish Institute of Human Rights. 2014. Myanmar Oil & Gas Sector-Wide Impact Assessment. Accessed March 4, 2021.

164 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples and land rights in Myanmar. Accessed March 4, 2021.

165 Socialist Republic of the Union of Burma. 1982. Burma Citizenship Law, Pyithu Hluttaw Law No. 4. Accessed March 8, 2021.

166 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples in Myanmar. Accessed March 4, 2021.

167 Myanmar Centre for Responsible Business, Institute for Human Rights and Business and Danish Institute for Human Rights. 2014. "Part 4.5: Project-level impacts: Ethnic Minority Groups / Indigenous Peoples" from Myanmar Oil & Gas Sector-Wide Impact Assessment. Accessed March 4, 2021.

168 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples in Myanmar. Accessed March 4, 2021.

169 Socialist Republic of the Union of Burma. 1982. Burma Citizenship Law, Pyithu Hluttaw Law No. 4. Accessed March 8, 2021.

170 Donna Guest. 2016. Briefing Paper: Indigenous Peoples' Rights and Business in Myanmar. Accessed March 8, 2021.

171 UPR. 2021. Coalition of Indigenous Peoples in Myanmar/Burma. Accessed May 21, 2021.

government, referring to all national races who have been present in the current geographical area of Myanmar since the earliest British annexation.<sup>172</sup>

The term “Indigenous Peoples” in Burmese is *hta-nay tain-yin-tha* (ဤနေထိုင်ရင်းသား), which translates as “original dwellers who have strong ancestral ties to the present territories”, based on the concept of self-identification.<sup>173</sup> However, it is not widely understood or generally used in Myanmar, except those who are working on ethnic rights and Indigenous rights.<sup>174</sup> Using this definition, Indigenous rights activists count more than 135 ethnic groups in Myanmar.<sup>175</sup> However ethnic groups are complex and politically sensitive and the majority of ethnic minorities believe that the government uses ethnic categories for political purposes; as those without legal recognition are unable to access otherwise internationally protected rights.<sup>176</sup>

Demographic processes have also impacted the recognition of Indigenous Peoples. The 2014 census suffered from methodological issues resulting in an undercount of approximately 1.2 million people.<sup>177</sup> This particularly impacted populations from certain northern zones in Rakhine State (home to the Rohingyas), and some villages in Kachin and Kayin States.<sup>178</sup> This institutional silencing has meant that Indigenous-driven narratives about their own realities remain unheard.

Thus, there is no accurate data about the actual population of Indigenous Peoples due to the insufficient recognition and restrictions on self-determination. In 2016, one count of the proportion of the population that are Indigenous was 32%.<sup>179</sup> Another count puts the non-Bamar population at 30-40% of the population.<sup>180</sup>

172 UPR. 2021. Coalition of Indigenous Peoples in Myanmar/Burma. Accessed May 21, 2021

173 UPR. 2021. Coalition of Indigenous Peoples in Myanmar/Burma. Accessed May 21, 2021

174 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples in Myanmar. Accessed March 4, 2021.

175 Myanmar Centre for Responsible Business, Institute for Human Rights and Business and Danish Institute for Human Rights. 2014. “Part 4.5: Project-level impacts: Ethnic Minority Groups / Indigenous Peoples” from Myanmar Oil & Gas Sector-Wide Impact Assessment. Accessed March 4, 2021.

176 Donna Guest. 2016. Briefing Paper: Indigenous Peoples’ Rights and Business in Myanmar. Accessed March 8, 2021.

177 IPUMS International. Sample Characteristics: Myanmar. Accessed March 10, 2021.

178 Minority Rights Group International. 2020. Myanmar/Burma. Accessed March 8, 2021.

179 Minority Rights Group International. 2020. Myanmar/Burma. Accessed March 8, 2021.

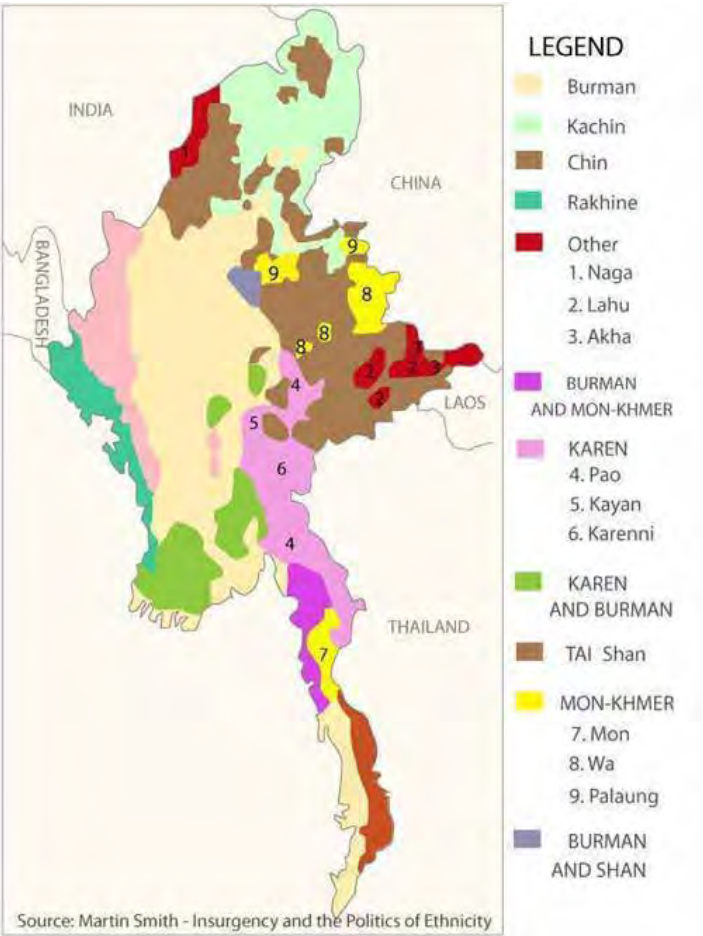
180 Donna Guest. 2016. Briefing Paper: Indigenous Peoples’ Rights and Business in Myanmar. Accessed March 8, 2021.



It is difficult to get an accurate and up to date sense of where Indigenous Peoples are located given government biases and flawed demographic processes. This map was chosen because it is relatively easy to read and understand. However, its accuracy is unverified, and it was originally published in 1991. It should be used with these limitations in mind. This map indicates ethnic groups in Myanmar. Territories and place names in Myanmar are contentious as self-determination rights are not upheld and largely undocumented.

Myanmar is broken up into 21 administrative subdivisions, including seven states, seven regions, five self-administered zones, one union territory and one self-administered division, divided generally by ethnic group. Kachin, Shan, Mon, Kayan, Kayin, Chin, Rakhine and Shan peoples are mostly located in their states. Burmans have no specific state but are the dominant population and are integrated into each of the seven regions (Sagaing, Magwe, Tanintharyi, Mandalay, Yangon, Ayeyarwady, and Bago).<sup>181</sup> There are also six self-administered areas that are part of Regions or States, each named after the national race that forms the majority in the relevant area (Naga, Danu, Pa-O, Palaung, Kokang and Wa). Naypyidaw Union Territory is where the Myanmar capital, Naypyidaw, is located. The majority of ethnic groups live in remote areas and highlands.

**Map of distribution of ethnic groups in Myanmar**



Original Source Retrieved from Radio Free Asia website at [https://www.rfa.org/english/news/myanmar/health-10192010185147.html/Burma\\_Ethnic\\_Map\\_500.jpg](https://www.rfa.org/english/news/myanmar/health-10192010185147.html/Burma_Ethnic_Map_500.jpg)

<sup>181</sup> Myanmar Centre for Responsible Business, Institute of Human Rights and Business and Danish Institute of Human Rights. 2014. Myanmar Oil & Gas Sector-Wide Impact Assessment. Accessed March 4, 2021.



## 2. Overview of the situation of IEHRDs

Indigenous Peoples in Myanmar have been fighting for their rights since Myanmar's independence in 1948. The policy of the 1962 military junta of "one religion, one culture, one language and one identity" impacted the stability of Indigenous Peoples in the country.<sup>182</sup> The military junta committed a wide range of human rights violations against Indigenous Peoples, including extra-judicial killings, torture, and forced labor.<sup>183</sup> Arrests of activists were regular while significant government censorship and deliberately controlled internet impacted access to information, freedom of expression, and human rights activities. This military junta ruled from 1962 until 2011.

In 2012, a quasi-civilian government was elected into power. Until this point, Myanmar was largely closed to the outside world. Subsequently, the country underwent a process of democratization and opening, including an economic overhaul aimed at attracting foreign investors. However, a culture of self-censorship has remained, and Indigenous Peoples continue to struggle for recognition and independence. State Counsellor Aung San Suu Kyi has been criticized for her inaction regarding the continued human rights violations against the Rohingya people, who have been targeted since 1978.<sup>184</sup>

At the core, IEHRDs in Myanmar are fighting for their land rights. Laws are regularly used to limit Indigenous Peoples' access to their rights. Most recently, this has been done through the 2012 Virgin Fallow and Vacant Land Management Law (VFV Land Law), which allows the government to take possession of unregistered land across the country. Myanmar lacks a functioning land cadastral system. Therefore, data and information on lands are inappropriately classified and unregistered, with the majority being in Indigenous territories. Approximately 75% of VFV land in the seven ethnic states have been extremely impacted.<sup>185</sup> Amendments to the law in 2019 disproportionately impacted Indigenous Peoples, requiring registration processes that remote-dwelling ethnic groups were unaware of, and were unable to meet due to inadequate support for documentation. Further, these processes are rooted in legal frameworks that Indigenous Peoples neither relate to nor trust. Paul Sein Twa, a Karen IEHRD, has also noted that Peace Parks, which seek to promote peace building by preserving biodiversity and Karen Indigenous cultural heritage, are threatened by the VFV Law.<sup>186</sup> Thus, in the absence of adequate land governance mechanisms and information, the law has been interpreted as a method that the government has used to take control of Indigenous territories.

Indigenous women are particularly impacted with regard to land rights. They often do not have land tenure rights due to discrimination. Some ethnic groups allow for land

- 
- 182 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples and land rights in Myanmar. Accessed March 4, 2021. Medha Chaturvedi. 2012. Myanmar's Ethnic Divide: The Parallel Struggle. Accessed March 8, 2021.
- 183 Myanmar Centre for Responsible Business, Institute of Human Rights and Business and Danish Institute of Human Rights. 2014. Myanmar Oil & Gas Sector-Wide Impact Assessment. Accessed March 4, 2021.
- 184 Open Observatory of Network Interference, Sinar Project and Myanmar ICT for Development Organization. 2017. The State of Internet Censorship in Myanmar. Accessed March 8, 2021.
- 185 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples and land rights in Myanmar. Accessed March 4, 2021.
- 186 Rina Chandran. 2020. Indigenous wisdom protects forests, says prize-winning Myanmar activist. Accessed May 19, 2021.

ownership by both men and women while others do not. They also face cultural, language, literacy, and geographical barriers. As a result, many Indigenous women do not possess written land deeds, and experience significant barriers in accessing such documentation.<sup>187</sup>

The Myanmar government began a digital transformation and released control over the development of communications infrastructure and technology in 2012. Limitations on internet service providers (ISPs) were removed, drastically decreasing the cost of access to the internet and dramatically increasing usage. With the increase of affordable smartphones in the last few years, internet usage in Myanmar has been at an all-time high. However, a rural-urban divide remains in terms of accessibility of information and communications technology (ICT), in which those living in rural areas typically lack the infrastructure, tools, and skills to go online.<sup>188</sup> Almost three-quarters of the population in Myanmar live in rural areas, with ethnic minorities over-represented in rural and remote areas.<sup>189</sup> One consequence of this is that information about Indigenous Peoples, from their own perspectives, is underrepresented online.

Human rights activism has also been transformed with the availability of online advocacy platforms via channels such as Twitter and Facebook. Digital platforms have become a principal tool for IEHRDs to express themselves and access information.<sup>190</sup> Thus, internet censorship has grown as a way to silence IEHRDs in Myanmar. While ISPs censorship was low in early 2017<sup>191</sup>, it has increased since, especially after the August 2017 military crackdown on Rohingya people. This crackdown has been considered a campaign to expand government territories on ethnic land.<sup>192</sup> Internet access in Rakhine State has been blocked since June 2019, and more than 200 webpages and several Indigenous news sites, on which Indigenous human right defenders have advocated on human rights, have been blocked.<sup>193</sup> Social media is increasing in importance during the current military coup, with users reporting higher levels of trust in this tool.<sup>194</sup> Free Expression Myanmar reports that digital freedom of expression in Myanmar has declined from 2018 to 2020 as shown in the table below.

187 Donna Guest. 2016. Briefing Paper: Indigenous Peoples' Rights and Business in Myanmar. Accessed March 8, 2021.

188 Freedom House. 2020. Freedom on the Net 2020: Myanmar. Accessed March 8, 2021.

189 Open Development Myanmar. 2016. Population and Censuses. Accessed March 8, 2021.

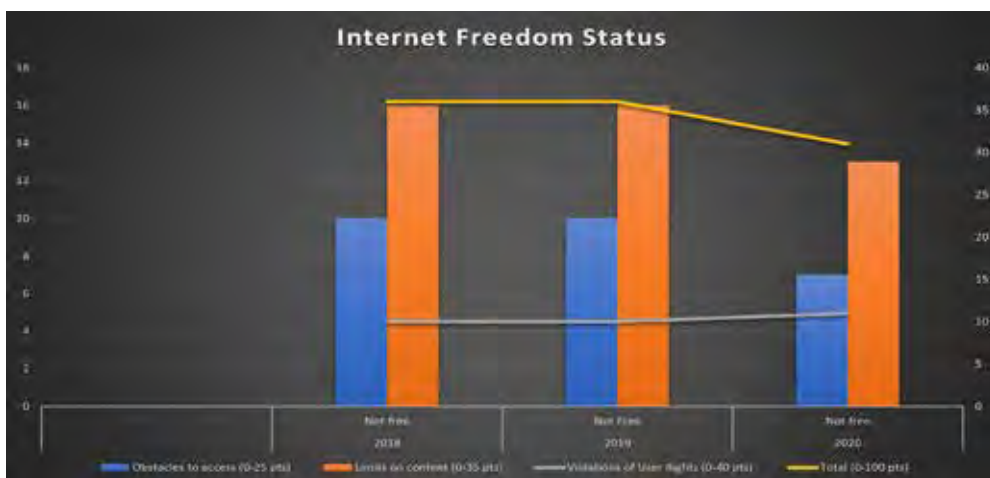
190 Freedom House. 2020. Freedom on the Net 2020: Myanmar. Accessed March 8, 2021.

191 Open Observatory of Network Interference, Sinar Project and Myanmar ICT for Development Organization. 2017. The State of Internet Censorship in Myanmar. Accessed March 8, 2021.

192 International Working Group on Indigenous Affairs. 2020. While the world focuses on COVID-19, Indigenous Peoples in Myanmar are being killed. Accessed March 3, 2021.

193 International Working Group on Indigenous Affairs. 2020. While the world focuses on COVID-19, Indigenous Peoples in Myanmar are being killed. Accessed March 3, 2021.

194 Mercedes Fogarassy, Catherine Barker and Shaelyn Laurie. 2021. Increased trust in social media following coup in Myanmar despite ongoing internet shutdowns. Accessed March 8, 2021.

**Figure:** Internet Freedom Status from 2018 to 2020

Source: Freedom House. 2020. Freedom on the Net 2020.

Since the start of the COVID-19 pandemic, critics have interpreted government actions as widespread shutting down of the freedoms of movement, assembly, and expression, as well as narrowing of access to information. Some have considered that the government is using the pandemic as an opportunity to stop human rights defenders. Despite the pandemic, the Myanmar authorities have increased their conflicts with the ethnic armed groups. Activist Naw Hser Hser, general-secretary of the Women's League of Burma, has said, "While the country is dealing with the COVID-19 pandemic, the military is escalating its offensives against ethnic armed groups in Rakhine, Chin, Karen and northern Shan states."<sup>195</sup> For example, 2,000 military troops were deployed in a Karen National Union (KNU)-controlled area of Karen State between January-April 2020. Villages were attacked to push the development of a strategic road, forcing the displacement of thousands of people.<sup>196</sup> The KNU is a Karen ethnic armed group that had signed a ceasefire agreement with the Myanmar military (Tatmadaw) in 2015.

Further, freedom of speech and information continues to be limited by policies that disproportionately impact Indigenous Peoples, regardless of officially provided justifications. Of particular note is the previously mentioned internet shutdown, from June 2019 until February 2021, in primarily ethnic nationality populated Rakhine and Chin States. Indigenous Peoples there were unable to access updated information on COVID-19, which significantly increased the risk of COVID-19 outbreaks, and also limited their ability to respond appropriately to the pandemic.

Although Myanmar has signed various international and regional declarations on protecting women's rights, including the UN Convention on the Elimination of Discrimination against Women (CEDAW), gender inequality is an ongoing struggle. Indigenous women are particularly marginalized. This is an institutional issue, as women and Indigenous Peoples are significantly underrepresented at all levels of administration. For instance, in the 330

195 International Working Group on Indigenous Affairs. 2020. While the world focuses on COVID-19, Indigenous Peoples in Myanmar are being killed. Accessed March 3, 2021.

196 International Working Group on Indigenous Affairs. 2020. While the world focuses on COVID-19, Indigenous Peoples in Myanmar are being killed. Accessed March 3, 2021.

municipalities of Myanmar, no municipal administrator is female. Of 16,785 Village Tract/Ward Administrators, only 42 (or 0.25%) are women.<sup>197</sup>

Deeply embedded gender biases impact women IEHRDs.<sup>198</sup> Myanmar is a deeply patriarchal society, and this has impacted the way that women are able to engage publicly. It has particularly impacted women's access to digital tools. Women are considered unable to use technology, and men act as the gatekeepers of technological tools, including computers and phones. Nor do women have access to the money necessary to purchase a phone and online access. This has limited their ability to use and access digital tools. They are less likely than men to own a smartphone or have the necessary skill to use it.<sup>199</sup>

Women IEHRDs are also more likely to suffer gender-based violence (GBV). Indigenous women are particularly at risk of sexual assault and rape by armed groups.<sup>200</sup> GBV extends to online interactions.<sup>201</sup> Women have no legal protections against online harassment and abuse.<sup>202</sup> Low knowledge of digital security measures to protect against hacking or phishing as well as high instances of online GBV such as cyberbullying has extended existing violence to online environments and contributes to the internet being a very unsafe space for Myanmar women.<sup>203</sup> Gender norms perpetuate this inequality.<sup>204</sup>

On February 1, 2021, the Tatmadaw staged a coup d'état, deposing newly re-elected State Counsellor of Myanmar Aung San Suu Kyi and imposing a year-long state of emergency. A number of actions led by the Tatmadaw recalling the time of the first military junta have since occurred. Those include arbitrary arrests of democracy activists and government leaders, imposition of a curfew, communications infrastructure shutdowns, and censorship of the press and internet. Significant changes to laws have been made, primarily limiting access to information and freedom of expression while also handing control of personal information to the military junta and increasing the severity of punishments.

The political situation in Myanmar continues to be volatile. Over the long term, it is expected that the situation for IEHRDs will get worse before it improves. Deliberate changes of law and policy around data and information clearly indicates a trend toward greater surveillance and direct persecution of activists. IEHRDs are likely to be specific targets due to the territories they occupy.

197 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples in Myanmar. Accessed March 4, 2021.

198 Mia Chung and Pyrou Chung. 2020. Mekong women in open data. Accessed March 8, 2021.

199 Mia Chung and Pyrou Chung. 2020. Mekong women in open data. Accessed March 8, 2021.

200 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples in Myanmar. Accessed March 4, 2021.

201 Mia Chung and Pyrou Chung. 2020. Mekong women in open data. Accessed March 8, 2021.

202 Myanmar Centre for Responsible Business. 2019. Third Myanmar Digital Rights Forum ends with call for better regulated, freer, safer online space, emphasises need for consultation. Accessed March 8, 2021.

203 Freedom House. 2020. Freedom on the Net 2020: Myanmar. Accessed March 8, 2021.

204 Mia Chung and Pyrou Chung. 2020. Mekong women in open data. Accessed March 8, 2021.

### 3. Methodology used for the formulation of the study

The methodology used for this study consists of desk research of the published and unpublished materials in English and Burmese. While the intention was to conduct key informant interviews with leaders in relevant Indigenous organizations, due to the current political situation in Myanmar, it was determined that it is unsafe to do so at this time. Thus, this study comprises only desk research.



Indigenous Woman in Chin State, Myanmar

## 4. Indigenous Environment Human Rights Defenders (IEHRDs) and Cybersecurity law and policies

### 4.1 Relevant international declarations, covenants, and other agreements

#### 4.1.1 CEDAW - Convention on the Elimination of All Forms of Discrimination against Women

Myanmar has acceded to CEDAW, an international treaty. It is intended to be an internationally recognized bill of rights for women. Despite this, the government has passed a number of laws that take away from the rights set out in this treaty, including the Buddhist Women's Special Marriage Law, the Population Control Healthcare Law and the Monogamy Law in 2015.<sup>205</sup>

#### 4.1.2 UNDRIP - United Nations Declaration on the Rights of Indigenous Peoples

Myanmar is a signatory to the UNDRIP. However, it has not implemented all of the rights provided in this declaration, including the right to self-determination. In particular, the term "Indigenous Peoples" as used in the declaration is not accepted in law, policy and practice. For instance, only certain groups are considered "national races" or "Indigenous", and other ethnic groups cannot identify as a "national race". Only "national races" can be "citizens", and only "citizens" receive constitutional protections. Further, Myanmar has not ratified ILO Convention No. 169.<sup>206</sup> Additionally, Free Prior and Informed Consent (FPIC)<sup>207</sup> of Indigenous Peoples for decision-making on matters affecting them has not been applied in Myanmar<sup>208</sup> and consultations with Indigenous Peoples remain limited.

#### 4.1.3 UDHR - Universal Declaration of Human Rights

Myanmar is a signatory to the UDHR, a declaration enshrining the rights and freedoms of all human beings. However, Myanmar is not a signatory to the covenant giving legal force to the UDHR, the International Covenant on Civil and

205 Shameema Rahman and Wendy Zeldin. 2015. Burma: Four "Race and Religion Protection Laws" Adopted. Accessed March 9, 2021. Amnesty International and International Commission of Jurists. 2015. Parliament must reject discriminatory 'race and religion' laws. Accessed March 8, 2021.

206 International Work Group for Indigenous Affairs. 2020. Indigenous Peoples in Myanmar. Accessed March 4, 2021.

207 General Assembly of the United Nations. 2007. United Nations Declaration on the Rights of Indigenous Peoples at Article 32. Accessed March 4, 2021.

208 Donna Guest. 2016. Briefing Paper: Indigenous Peoples' Rights and Business in Myanmar. Accessed March 8, 2021.

Political Rights (ICCPR). Issues have also arisen with regard to the wording of some Myanmar laws. For instance, Human Rights Watch has noted that Article 66(d) of the Telecommunications Law (2014) is written in a way that is too broad and vague to be in accordance with the requirements of the UDHR.<sup>209</sup>

#### 4.1.4 ICESCR – International Covenant on Economic, Social and Cultural Rights

The International Covenant on Economic, Social and Cultural Rights (ICESCR) is a multilateral treaty adopted by the United Nations General Assembly on 16 December 1966, and in force from 3 January 1976. Myanmar signed the Treaty in July 2015 and ratified it in October 2017.<sup>210</sup>

## 4.2 Laws

This section analyzes the laws, including with regard to government agencies and the roles they play in the implementation of the laws; specific provisions that impact the human rights of IEHRDs; any protections or penalties for violation of the provisions of the law; and how the law caters to gender, if at all. Relevant policies and court cases are discussed in context.

A number of laws both directly and indirectly related to cybersecurity impact IEHRDs in Myanmar. These include the following:

- Constitution of the Republic of Myanmar (2008)
- Ethnic Rights Protection Law or the Protection of the Rights of National Races Law (2015)
- Draft Cybersecurity Bill (2021)
- Electronic Transactions Law (2004, amended 2021)
- Telecommunications Law (2013)
- Law Protecting the Privacy and Security of Citizens (2017, August 2020)
- Draft Right to Information Bill (2016)
- Myanmar Penal Code (1861)

These laws primarily limit freedoms without providing any framework for security, data management, or intellectual property. Nor is gender mainstreamed into those laws or Myanmar's legal and policy framework in general. Gender is discussed in the 2008 Constitution, and there is a draft Violence against Women law. However, the critics indicate that this draft law still does not meet international standards.<sup>211</sup>

209 Human Rights Watch. 2017. Burma: Repeal Section 66(d) of the 2013 Telecommunications Law. Accessed March 8, 2021.

210 ICJ. 2018. ICJ and Myanmar National Human Rights Commission Forum on Economic, Social and Cultural Rights. Accessed May 21, 2021.

211 Global Justice Centre Blog. 2020. Myanmar's Proposed Prevention Of Violence Against Women Law - A Failure to Meet International Human Rights Standards. Accessed March 8, 2021.



## 4.2.1 Constitution of the Republic of Myanmar (2008)

The Constitution sets out the basic principles of the Republic of Myanmar<sup>212</sup>; the democratic structure<sup>213</sup>; defense services<sup>214</sup>; rights and duties of the citizens<sup>215</sup>; the political structure<sup>216</sup>; emergency provisions<sup>217</sup>; procedure to amend the Constitution<sup>218</sup>; state flag, seal, anthem and capital<sup>219</sup>; and transitory and general provisions<sup>220</sup>.

Chapter 8<sup>221</sup> of the Constitution is one of the few provisions in Myanmar laws or policies where gender equality is mentioned.<sup>222</sup> However, gender equality is limited; for instance, there is to be no discrimination in civil service, except that some positions may be suitable for men only.<sup>223</sup> Further, women and men are intended to have equal access to acquiring, retaining and conferring their nationality<sup>224</sup>; however, women's citizenship rights are subject to practical and customary constraints. All persons in Myanmar are to have equal rights under the law<sup>225</sup>, and there should be no discrimination by sex, race, birth, religion and other characteristics<sup>226</sup>.

Ethnic rights in Myanmar also have limited protection under the 2008 Constitution. Article 365 provides for the right of Myanmar citizens to freely develop literature, culture, arts, customs and traditions “that they cherish”, but only if it is not detrimental to national solidarity. Further, “any particular action which might adversely affect the interests of one or several other national races shall be taken only after coordinating with and obtaining the settlement of those affected”.

Further, all citizens are guaranteed the right to freedom of expression among other rights<sup>227</sup>, but only if it is “not contrary to the laws, enacted for Union security, prevalence of law and order, community peace and tranquility or public order and morality”. These provisions indicate that the government keeps significant restrictions to these rights, because “public order”, “community peace”, and “national solidarity” are not defined.

Additionally, Article 357 is of particular interest, which states that “the Union must protect the privacy and security of home, property, correspondence and other communications of citizens under the law subject to the provisions of the Constitution”. There is a 2017 Law Protecting the Privacy and Security of Citizens which further clarifies the Constitutional protection.

- 
- 212 The Constitution of the Republic of Myanmar. 2008. Chapter 1. Accessed March 8, 2021.
  - 213 The Constitution of the Republic of Myanmar. 2008. Chapters 2-6. Accessed March 8, 2021.
  - 214 The Constitution of the Republic of Myanmar. 2008. Chapter 7. Accessed March 8, 2021.
  - 215 The Constitution of the Republic of Myanmar. 2008. Chapter 8. Accessed March 8, 2021.
  - 216 The Constitution of the Republic of Myanmar. 2008. Chapters 9-10. Accessed March 8, 2021.
  - 217 The Constitution of the Republic of Myanmar. 2008. Chapter 11. Accessed March 8, 2021.
  - 218 The Constitution of the Republic of Myanmar. 2008. Chapter 12. Accessed March 8, 2021.
  - 219 The Constitution of the Republic of Myanmar. 2008. Chapter 13. Accessed March 8, 2021.
  - 220 The Constitution of the Republic of Myanmar. 2008. Chapters 14 and 15. Accessed March 8, 2021.
  - 221 The Constitution of the Republic of Myanmar. 2008. Articles 345-390. Accessed March 8, 2021.
  - 222 The Constitution of the Republic of Myanmar. 2008. Arts. 350 and 351. Accessed March 8, 2021.
  - 223 The Constitution of the Republic of Myanmar. 2008. Art. 352. Accessed March 8, 2021.
  - 224 The Constitution of the Republic of Myanmar. 2008. Arts. 345 – 355. Accessed March 8, 2021.
  - 225 The Constitution of the Republic of Myanmar. 2008. Art. 347. Accessed March 8, 2021.
  - 226 The Constitution of the Republic of Myanmar. 2008. Art. 348. Accessed March 8, 2021.
  - 227 The Constitution of the Republic of Myanmar. 2008. Art. 354a. Accessed March 8, 2021.

## 4.2.2 Ethnic Rights Protection Law or the Protection of the Rights of National Races Law (2015)

The 2015 Protection of the Rights of National Races Law includes as one of its purposes “to aim for the socio-economic development of less-developed national races including education, health, economics and transportation”.<sup>228</sup> While the law discusses providing equal rights to all national races<sup>229</sup>, it does not actually provide any protection from discrimination. Further, it has been reported that Indigenous Peoples were not consulted in the development of this law.<sup>230</sup> This law lacks clarity. The word “Indigenous Peoples” (hta-nay tain-yin-tha) is used in this law, but it is undefined, and does not appear in any other laws.<sup>231</sup>

## 4.2.3 Draft Cybersecurity Bill (2021) and Electronic Transaction Law (2004, amended 2014 and 2021)

ICT and cybersecurity have been of interest to the government of Myanmar, beginning with the government signing the e-ASEAN Framework Agreement in 2000. The purpose of this agreement was to initiate ASEAN’s effort to bridge the digital divide with the rest of the world, with each other, and within their respective countries.<sup>232</sup>

Cybersecurity increased in importance after the Distributed Denial of Service attacks that disrupted the network prior to the 2010 Myanmar General Election. Subsequently, a Cybersecurity Steering Committee was formed. The government began drafting a number of technology-related master plans in 2015, including an E-Government Master Plan and a Telecommunications Master Plan. The E-Government Master Plan was adopted and was in place from 2016-2020; a second plan for 2021-2025 was expected prior to the February 2021 coup d’état.<sup>233</sup> The Telecommunications Master Plan has not yet been adopted.

In 2015, the Information Technology and Cyber Security Department (ITCSD) was formed under the Ministry of Transportation and Communication (MoTC). Under the ITCSD, a National Cyber Security Center (NCSC) has been established, with the mandate to provide online services securely and to provide access to e-government and other online services safely. The Myanmar Computer Emergency Response Team (mmCERT) was formed in 2004, and the UN Security Operation Centre supports the work of the NCSC.

However, the legal framework governing cybersecurity - including personal data protection; critical information infrastructure protection; response and investigation of cyber threats; service provider and computer misuse; and cybercrimes - does not protect Myanmar’s citizens. Relevant laws have been used more to criminalize

228 Protection of the Rights of National Races Law. Article 3(e). Accessed March 8, 2021.

229 Protection of the Rights of National Races Law. Article 3(e). Accessed March 8, 2021.

230 Donna Guest. 2016. Briefing Paper: Indigenous Peoples’ Rights and Business in Myanmar. Accessed March 8, 2021.

231 Donna Guest. 2016. Briefing Paper: Indigenous Peoples’ Rights and Business in Myanmar. Accessed March 8, 2021.

232 ASEAN. 2000. e-ASEAN Framework Agreement. Accessed March 8, 2021.

233 Salai Tun Tun. 2020. Second Myanmar e-governance master plan to include systems for cyber-crime, e-payments. Accessed March 8, 2021.

users than to protect them. Those laws include the Electronic Transaction Law (2004, amended in 2014 and 2021) and the Draft Cybersecurity Bill (2021).

The Electronic Transaction Law was adopted in 2004. The stated objectives of the Law are to support with developing electronic transactions technology; to obtain more opportunities for development of sectors; recognize the authenticity and integrity of electronic record and electronic data message and give legal protection; to enable online transmitting, receiving and storing local and foreign information; and enable online communicating and co-operating effectively and speedily (Article 3). However, the law has been used primarily to regulate devices and control phone and internet users with harsh criminal punishments.<sup>234</sup> The military junta passed an amended Electronic Transaction Law on February 15, 2021 without forewarning or opportunity to consult. These amendments used significant content from the 2021 draft Cybersecurity Bill.

A draft Cybersecurity Bill was first introduced in 2019<sup>235</sup>, but it was abandoned. The 2021 military junta introduced a new draft cybersecurity bill in 2021, which received widespread condemnation both by local CSOs<sup>236</sup> and international observers<sup>237</sup> due to its impact on human rights, particularly freedom of expression. While this bill has not yet been passed, the 2021 amendment to the Electronic Transaction Law copies much of the text from the draft Cybersecurity Bill. If the draft Cybersecurity Bill does eventually get passed, it will completely repeal the Electronic Transaction Law.<sup>238</sup> Thus, we include an analysis of some of the provisions in this bill that have not been included in the amendment to the Electronic Transactions Law to indicate some potential future risks to IEHRDs.

#### 4.2.4 Electronic Transactions Law

The 2021 amendments have expanded the definitions section, including by defining personal information, the person responsible for management of personal information, cyber resources, cyberspace, and cyber-attack.<sup>239</sup> This is from the draft cybersecurity bill. The amendments have also included a new objective, “to protect the personal information of the public in accordance with the law”.<sup>240</sup>

The amendments include an additional Chapter (10) on “Protection of Personal Information”, but critics have indicated that the provisions are very poorly defined, and that the exceptions to protection granting authorities broad powers may undermine any protections these provisions provide.<sup>241</sup> The exceptions that may potentially impact IEHRDs in a disproportionate manner are regarding investigations related to

234 Free Expression Myanmar. 2017. Electronic Transactions Law. Accessed March 8, 2021.

235 Myanmar Cyber Law (Draft) 2019: Abandoned. Accessed March 8, 2021.

236 Free Expression Myanmar. 2021. Six risks from Myanmar’s draft cybersecurity law. Accessed March 8, 2021.

237 Human Rights Watch. 2021. Myanmar: Scrap sweeping cybersecurity bill. Accessed March 8, 2021.

238 Free Expression Myanmar. 2021. Myanmar’s new Electronic Transactions Law Amendment. Accessed March 8, 2021. See Article 89 of the law.

239 Pyidaungsu Hluttaw. Law Protecting the Privacy and Security of Citizens, Union Parliament Law 5/2017, as amended by Law 16/2020. Accessed March 8, 2021.

240 Pyidaungsu Hluttaw. Law Protecting the Privacy and Security of Citizens, Union Parliament Law 5/2017, as amended by Law 16/2020 at s.3f. Accessed March 8, 2021.

241 Free Expression Myanmar. 2021. Myanmar’s new Electronic Transactions Law Amendment. Accessed March 8, 2021.

collecting information “carried out under the authority of respective criminal case”<sup>242</sup> and investigation and collecting information “carried out in accordance with the authority on each relevant issue of stability of state sovereignty, public order, national security [when] the cybersecurity and cybercrime [fall under those aforementioned issues]”<sup>243</sup>. The provisions have not yet been used. However, it could potentially apply to IEHRDs under investigation under the Penal Code’s “public tranquility” or “sedition” provisions (or other criminal investigations). Since the provisions are so broad, there is the potential that very personal data, including social media activities or private online communications, would be subject to collection without any warning.<sup>244</sup>

In addition, of particular interest to IEHRDs is section 33b of the 2004 Electronic Transaction Law, which forbids the sending or distribution of “information relating to secrets of the security of the state” online. This provision is worded very broadly and has been applied to communications about cultural or economic affairs. It has been used to imprison journalists, bloggers and activists, most notably in 2008 to impose sentences of up to 65 years on activists, bloggers, and members of the 88 Generation Students Group.<sup>245</sup> This article remains as is.

The amendments also have added a number of new punishments for online activities, including “creating misinformation and disinformation with the intent of causing public panic, loss of trust or social division on Cyberspace”.<sup>246</sup> This is punishable by imprisonment for a term of 1 to 3 years, or a fine not exceeding 50 lakhs MKR, or both.<sup>247</sup><sup>81</sup> This text is from the draft cybersecurity bill. The wording is very vague and broad and is not clearly defined.

## 4.2.5 Draft Cybersecurity Bill

On February 9, the military government introduced a draft Cyber Security Law (CSL) and February 15, SAC announced CSL as an illegitimate amendment to the Electronics Transactions Law without warning.<sup>248</sup> The provisions in the draft Cybersecurity Bill giving the military’s State Administration Council control over the internet and data were not included in the amendments to the Electronic Transactions Law. Some of these draft provisions are analyzed below.

The draft Cybersecurity Bill would require “online service providers” to collect and store user data for three years and provide this information at request.<sup>249</sup> Online service provider is vaguely defined, but has usually meant an online news provider, entertainment provider, social media site or newsgroup. Online services are required to be registered<sup>250</sup>, and the government may be able to remove any

242 2021. Amended Electronic Transactions Law at s.27c(2). Accessed March 8, 2021.

243 2021. Amended Electronic Transactions Law at s.27c(3). Accessed March 8, 2021.

244 Free Expression Myanmar. 2021. Myanmar’s new Electronic Transactions Law Amendment. Accessed March 8, 2021.

245 Jonathan Head. 2008. Harsh sentences for Burma rebels. Accessed March 8, 2021.

246 2021. Amended Electronic Transactions Law at s.38c. Accessed March 8, 2021.

247 Pyidaungsu Hluttaw. Law Protecting the Privacy and Security of Citizens, Union Parliament Law 5/2017, as amended by Law 16/2020 at s.3f. Accessed March 8, 2021.

248 Thomas H. Andrews. 2021. Report of the Special Rapporteur on the situation of human rights in Myanmar. Accessed May 24, 2021

249 2021. Draft Cybersecurity Law at para 30-31. Accessed March 8, 2021.

250 2021. Draft Cybersecurity Law at para 34. Accessed March 8, 2021.

information it deems “misinformation or disinformation”<sup>251</sup>, visit the online services’ place of business<sup>252</sup>, and be granted access to data and systems for the purposes of conducting an investigation of an alleged threat, fraud, crime, or “cyber incident”<sup>253</sup>, or shut down the provider to safeguard the public interest<sup>254</sup>. The provisions do not require notice, warrant, or judicial oversight. These provisions severely limit freedom of expression and place the personal security of IEHRDs at risk if they engage in any online advocacy.

#### 4.2.6 Telecommunications Law (2013, amendment 2017)

The Telecommunications Law was introduced in 2013 by the former President Thein Sein’s government and amended in 2017. Currently, the Telecommunications Department under the Ministry of Transport and Communications (MOTC) is responsible for the implementation of this law. The stated objectives of the Law are related to regulating the development, expansion and provision of telecommunications services in the country<sup>255</sup> as well as the protection of providers and users<sup>256</sup> and the supervision of the provision of services<sup>257</sup>. However, the provisions related to protection and supervision of the provision of telecommunications give the responsible government agency significant powers<sup>258</sup> to ensure the “stability and security of the country”<sup>259</sup>, prevent “harm to security, law, and peace”<sup>260</sup>, and for “the benefit of the people”<sup>261</sup>. These terms are not defined in the law. Further, there are no safeguards in the public interest.<sup>262</sup>

In reality, this law has been used to restrict the freedom of online expression of human rights activists. “The Telecommunications Law was aimed to regulate telecommunications, but it is being used as a weapon to control the media,” said Kyaw Min Swe, chief editor of The Voice Daily.<sup>263</sup> One article of potential relevance to IEHRDs is Article 68(a), which criminalizes maliciously communicating false information. Other provisions of the law have specifically been used to criminalize human rights activists. Article 66(d) of this law has particularly been used in this way, which states that:

*“Anyone found guilty of extorting, coercing, restraining, wrongfully defaming, disturbing, causing undue influence or threatening any person by using any telecommunications network shall be punished with a maximum three years in prison, a fine or both.”*

251 2021. Draft Cybersecurity Law at para 29b. Accessed March 8, 2021.

252 2021. Draft Cybersecurity Law at para 50. Accessed March 8, 2021.

253 2021. Draft Cybersecurity Law at paras 43 and 44. Accessed March 8, 2021.

254 2021. Draft Cybersecurity Law at para 51. Accessed March 8, 2021.

255 2013. Telecommunications Law at Article 4(a), (b), and (c). Accessed March 8, 2021.

256 2013. Telecommunications Law at Article 4(d)

257 2013. Telecommunications Law at Article 4(e)

258 2013. Telecommunications Law at Articles 18, 40, 75-77.

259 2013. Telecommunications Law for example Article 4 and 18.

260 2013. Telecommunications Law for example Articles 75-76.

261 2013. Telecommunications Law for example Article 77.

262 Free Expression Myanmar. 2017. Electronic Transactions Law. Accessed March 8, 2021

263 Human Rights Watch. 2019. Dashed hopes, the criminalization of peaceful expression in Myanmar. Accessed March 4, 2021.

The defamation aspect of this article was used in June 2020 to charge and arrest Htun Htun Oo, a human rights activist and leader of a Patheingyi-based organization for criticizing the military online. The burden of proof under this provision is high, and so especially impacts IEHRDs.<sup>264</sup>

Women IEHRDs are more likely to suffer disproportionately under this provision. The ability of women IEHRDs to make themselves heard is already quite limited, as they are more frequently excluded from social interactions, decision-making and development activities in Myanmar.<sup>265</sup> For women activists who do speak out, especially online, they are more likely to face gender-based attacks, due to a highly patriarchal society, militarization, and extremism.<sup>266</sup> Not only is this Telecommunications Law frequently used against IEHRDs, it also does not protect against gender-based harassment or abuse.

For example, Wai Wai Nu, a Rohingya woman human rights defender and the founder and director of Women Peace Network, has frequently experienced gender-based threats and violence online, receiving comments expressing violence against her as a woman and referring to her ethnicity in derogatory terms.<sup>267</sup> Her personal security is threatened, even as she has no legal recourse or protection, despite the fact that the Telecommunications Law is intended to protect users of telecommunications services.<sup>268</sup>

Article 77 of the Telecommunications Law, which gives the MOTC the authority to cut off a telecommunications service in an “emergency” situation, was used by the Myanmar government as the basis of the longest internet shutdown in the world. Referring to the Law, the MOTC stopped mobile internet traffic on June 21, 2019 in Rakhine and Chin States due to “disturbances of peace and use of internet services to coordinate illegal activities”.<sup>269</sup> Access was cut until February 3, 2021.

The Rakhine and Chin States are home to many Rohingya, an ethnic group in Myanmar. Armed conflict has been ongoing since 2017 in these states, centered around the right of self-determination of the Rohingya. The internet shutdown has meant that humanitarian organizations have been unable to coordinate assistance to those in need in the region, and during the COVID-19 pandemic has meant that some communities have not received information about this public health emergency and thus have limited ability to protect themselves.<sup>270</sup> This shutdown has not only limited the right of those living in these states to access information and express themselves, it has also significantly decreased their safety and security.

Article 77 was also used in March 2020 to block 221 websites, citing as justification that this was in response to “fake news” and misinformation about COVID-19.<sup>271</sup> These banned sites included ethnic news media as well as the websites of the organizations of human rights defenders, such as Justice for Myanmar.<sup>272</sup> This

264 Human Rights Watch. 2019. Dashed hopes, the criminalization of peaceful expression in Myanmar. Accessed March 4, 2021.

265 Freedom House. 2020. Freedom on the Net 2020: Myanmar. Accessed March 8, 2021.

266 Free Expression Myanmar. 2018. Daring to defy Myanmar’s patriarchy. Accessed March 4, 2021.

267 Arrow. 2021. Gender perspectives needed for rights to free speech. Accessed March 8, 2021.

268 2013. Telecommunications Law at Article 4.

269 Telenor Group. 2019. Network shutdown in Myanmar, 21 June 2019. Accessed March 8, 2021.

270 Human Rights Watch. 2020. Myanmar: End World’s Longest Internet Shutdown. Accessed March 8, 2021.

271 Article 19. 2020. Myanmar: Immediately Lift Ban on Ethnic News Websites. Accessed March 8, 2021.

272 Freedom House. 2020. Freedom on the Net 2020: Myanmar. Accessed March 8, 2021.



censorship exacerbates earlier action by Facebook, which since 2018 has removed a number of Facebook pages of Rohingya armed groups<sup>273</sup>, designating them “dangerous organizations”. These groups were subsequently defined as “terrorist organizations” by the Myanmar government.<sup>274</sup> While there is no overt evidence that Facebook was acting with a pro-regime bias, their actions imply it.<sup>275</sup>

A further, broader concern is with regard to access to information. A 2018 UN Fact Finding Mission indicated that for most users [in Myanmar], Facebook is the internet”.<sup>276</sup> Facebook censorship thus makes unavailable the most, and for many, the only accessible tools of expression for IEHRDs. This censorship is not limited to company-led bans; there have been reports by human rights defenders, particularly women and Indigenous activists, that they have been subjected to violence or threats intended to force them to remove their own content on social media, especially Facebook.<sup>277</sup>

#### 4.2.7 Law Protecting the Privacy and Security of Citizens (2017), amended in 2020, 2021.

This law is informally known as the “Privacy Law”. When the law came into force in 2017, observers noted that Article 8(f), which makes defamation a non-bailable offense, was overbroad and harsh. This provision has been used to squash criticism of the state, state leaders, and authorities since its coming into force.<sup>278</sup> The 2020 amendments retained the harsh sentence but modified the wording penalizing “whoever” is found guilty of s.8(f) to “any responsible authority”, clarifying that this law is intended to protect citizens from intrusions of the government.<sup>279</sup> However, privacy protections in this law have been suspended by the military junta.<sup>280</sup> This means that authorities may now enter premises, open private correspondence, or intercept electronic communications, among other things, all without a warrant.

On February 13, 2021, after the military seized power for less than two weeks, the Law Protecting the Privacy and Security of Citizens (2017) was amended by the State Administration Council (SAC).<sup>281</sup> These amendments chiefly address the power of the government to conduct searches, seizures, and arrests; to extend detention without judicial oversight; and to carry out broad surveillance and investigation activities that could intrude on individual privacy.<sup>282</sup> Various basic protections such as

273 This includes groups such as the Arakan Rohingya Salvation Army (ARSA), Arakan Army, Myanmar National Democratic Alliance Army, Kachin Independence Army, and Ta’ang National Liberation Army.

274 Angshuman Choudhury. 2020. How Facebook is complicit in Myanmar’s attacks on minorities. Accessed March 8, 2021.

275 See The Dirty List, a February 2021 document that shows the companies that have funded the Tatmadaw, which includes Facebook.

276 UN Human Rights Council. 2018. Myanmar: UN Fact-finding mission releases its full account of massive violations by military in Rakhine, Kachin and Shan States. Accessed March 8, 2021.

277 Freedom House. 2020. Freedom on the Net 2020: Myanmar. Accessed March 8, 2021.

278 San Yamin Aung. 2020. Myanmar amends privacy law to protect citizens from state intrusion. Accessed March 8, 2021.

279 Pyidaungsu Hluttaw. Law Protecting the Privacy and Security of Citizens, Union Parliament Law 5/2017, as amended by Law 16/2020 at s.3f. Accessed March 8, 2021.

280 The Irrawaddy. 2021. Myanmar military junta suspends laws protecting citizens’ privacy to crack down on opposition. Accessed March 8, 2021

281 The Global New Light of Myanmar. 2021. Amendment of Law Protecting the Privacy and Security of the Citizens. Accessed May 28, 2021

282 Clyde & Co LLP. 2021. Myanmar Amends Legislation on the Privacy and Security of Citizens

the right to be free from arbitrary detention, warrantless surveillance and seizure was removed. This amendment will be executed as long as the SAC is in power. Since 1 February, the military government arbitrarily detained over 1,200 individuals including human right defenders and interred the private residence for the purpose of searching, seizure, and arrest.<sup>283</sup>

#### 4.2.8 Right to Information Bill (2016)

The Right to Information Bill was proposed in 2016 just before the National League for Democracy (NLD) took power. While those consulted proposed a number of revisions to address some weaknesses<sup>284</sup>, the introduction of this bill was considered a positive step in the direction of government transparency<sup>285</sup>. However, this bill has not yet been adopted, which means that the citizens of Myanmar continue to have no legal path to seek rightful information and keep their government accountable.

#### 4.2.9 Myanmar Penal Code (1861)

The Myanmar Penal Code (1861) is a colonial law that is still in use today. The provisions are considered vague and overbroad, such that they can be easily used to suppress dissent and punish those who speak critically of the government.<sup>286</sup> Of particular concern to IEHRDs are provisions on sedition<sup>287</sup>, defamation<sup>288</sup>, and public tranquility<sup>289</sup>. The military junta has introduced amendments to the provisions on sedition and high treason<sup>290</sup> that broaden the provisions, and have also introduced new vaguely worded offences, including one relating to knowingly spreading “fake news”.<sup>291</sup> These amendments are considered by watchdog groups to be a preparation for a “sustained assault on freedom of expression”.<sup>292</sup>

---

amid State of Emergency. Accessed May 24, 2021

283 Thomas H. Andrews. 2021. Report of the Special Rapporteur on the situation of humanrights in Myanmar. Accessed May 24, 2021

284 UNESCO. 2016. UNESCO facilitates consultation on Right to Information law in Myanmar. Accessed March 8, 2021.

285 UNESCO. 2016. UNESCO facilitates consultation on Right to Information law in Myanmar. Accessed March 8, 2021.

286 Free Expression Myanmar. 2017. Penal Code. Accessed March 8, 2021.

287 1861. Myanmar Penal Code at s.124a. Accessed March 8, 2021.

288 1861. Myanmar Penal Code at s.499-502. Accessed March 8, 2021.

289 1861. Myanmar Penal Code at s.505b. Accessed March 8, 2021.

290 1861. Myanmar Penal Code at s.121. Accessed March 8, 2021.

291 Article 19. 2021. Myanmar: Penal Code amendments portend long-term repression. Accessed March 8, 2021.

292 Article 19. 2021. Myanmar: Penal Code amendments portend long-term repression. Accessed March 8, 2021.

This law has been known to be used against human rights defenders. Naw Ohn Hla, a well-known Indigenous Karen woman human rights defender and the chair of the Myanmar-based Democracy and Peace Women Network, has been imprisoned more than 20 times for criticizing the government's approach to ethnic minorities, widespread land grabbing, and systematic violations of women's rights ([Frontier Myanmar, 2019](#)). Section 505b of the Penal Code was used for at least two of these charges, including in 2013 and again in 2015.



Naw Ohn Hla, a well-known Indigenous Karen woman human rights defender.  
Original Source: <https://crd.org/2020/12/10/civil-rights-defender-of-the-year-2020-naw-ohn-hla/>

## 5. Recommendations

In this section, we discuss some recommendations based on our research. Ideally, these recommendations would be informed by key informant interviews and on-the-ground realities of IEHRDs. However, given the current political situation in Myanmar, we were unable to do so.

### Recommendation 1: Integrating the approach of state and non-state actors

#### 1.1. Accessible and affordable access to internet connectivity is a basic requirement.

The majority of Indigenous Peoples in Myanmar live in remote areas where there is poor to no internet connectivity. This limits their access to digital platforms that could be used by IEHRDs to advocate for their rights. Affordability of smartphones, credit and data packages are another obstacle out of reach for most but particularly for Indigenous women in rural areas. Digital transformation has allowed for new ways for people to connect to each other, but IEHRDs have limited access to these tools to access and disseminate information or for advocacy purposes. As a result, Indigenous issues, particularly those relating to Myanmar, remain underrepresented online and throughout the region.

**1.2. Digital literacy capacity building** should be a priority to ensure that IEHRDs are able to access their digital rights, which are an extension of human rights. This includes learning to use digital tools to support human rights advocacy. IEHRDs may also benefit from **training on rights**. Training should be conducted **using appropriate languages and materials** (e.g., audio, video, visual and not just written) with trusted local facilitators. Multiple sessions may be required to ensure that all members of the community can attend, and **women-only sessions** may be necessary to ensure that women's needs are met, and women's voices are heard.

**1.3.** For those interested in **exercising their right to protest**, [here](#) is a useful resource for understanding one's rights. It is available in Burmese and English, as well as other languages.

**1.4.** Citizens, CBOs, and NGOs should work together to **document and publish information** that would support advocacy, using **responsible data governance frameworks**. For communities of IEHRDs and the organizations supporting them, this includes following the **CARE principles** of Indigenous Data Sovereignty. This is a framework that supports Indigenous Peoples to retain control over the production, collection, use and distribution of data about themselves. Examples of documentation and data collection processes can include community mapping, video storytelling to document cultural practices, and creating a community dictionary of local plants and herbs.

**1.5.** Private sector should **follow the UN Guiding Principles on Business and Human Rights**, which requires that businesses should respect internationally recognized human rights, regardless of what the state obligates them to do. This includes complying with the standards set out in UNDRIP.<sup>293</sup>

293 Donna Guest. 2016. Briefing Paper: Indigenous Peoples' Rights and Business in Myanmar. Accessed March 8,

**1.6.** When developing policies, laws, programs and projects that may impact Indigenous Peoples, the government and private sector should **conduct regular and direct consultations** with Indigenous Peoples in order to obtain their FPIC. All consultations should use relevant local languages and be held in convenient locations for communities, and at multiple times to ensure maximum attendance. Sufficient time must be provided to ensure that there is true understanding of the issues at hand. To ensure that women's voices are heard, women-only sessions are necessary.

## Recommendation 2: Freedoms of expression and access to information

### 2.1. No more internet shutdowns.

Since June 2019, Indigenous Peoples in Rakhine State have had the longest government-mandated internet shut down in history. This had a significant impact upon the COVID-19 pandemic which contributed to a humanitarian crisis, increasing the strain upon healthcare services in the region as well as reducing access to health information during a pandemic making it hard to effectively respond to the crisis.<sup>294</sup> Currently the military junta seizure of power on February 1, has resulted in amended laws and regulations that restrict freedoms of expression and access to information even further. This is proactively exercised through disconnections and limitations to internet services as well as censorship and restrictions placed upon websites and access to social media platforms more broadly.<sup>295</sup>

Without restoration of ICT services human rights defenders in particular are at greater risks of increased persecution at the hands of the military government.<sup>296</sup> More than 700 civilians have been killed since the coup<sup>297</sup> and the scale of the pandemic is currently unknown, thus without internet access there is limited avenues for the dissemination of information in or out of the country. Fewer options to access current news and information on the current state of the human rights defenders as well as critical information on pandemic controls. This practice of internet shutdown and censorship needs to stop and all services and access restored to everyone equally.

### 2.2. Freedoms of expression should be upheld according to international standards.

Since 2011, freedom of expression in Myanmar had seen signs of improvement yet unfortunately has deteriorated under the recent seizure of power by the Junta. Several laws such as Electronic Transactions Law (2004, amended 2021), Telecommunications Law (2013), and Myanmar Penal Code (1861) greatly limit freedom of expression to online users.<sup>298</sup> Specifically, these amendments are against Article 19 of the Universal Declaration of Human Rights protects the right to freedom of expression. Under this convention everyone has the right to hold opinions without interference and the right to freedom of expression, including the freedom to seek, receive and impart information.

2021. James Anaya. 2013. Report of the UN Special Rapporteur on the Rights of Indigenous Peoples at p. Accessed March 8, 2021.

294 Amnesty International. 2021. Myanmar: New internet blackout "heinous and reckless". Accessed May 28, 2021.

295 Andrea Januta and Minami Funakoshi. 2021. Myanmar's internet suppression. Accessed May 28, 2021.

296 Amnesty International. 2021. Myanmar: New internet blackout "heinous and reckless". Accessed May 28, 2021.

297 BBC. 2021. Myanmar coup: The people shot dead since the protests began. Accessed May 28, 2021.

298 Thomas H. Andrews. 2021. Report of the Special Rapporteur on the situation of human rights in Myanmar. Accessed May 24, 2021

The government should retract all such laws which violate the rights to freedoms of expression and adopt a national action plan incorporating a wide range of policy measures consistent with international standards and best practices stated Article 19.<sup>299</sup> Additionally, online hate speech and disinformation against Indigenous Peoples and minority groups, predominantly perpetrated by the State actors themselves needs to desist.<sup>300</sup>

### **2.3. The rule of law, democracy and protection of the rights, privacy and security of people in Myanmar needs to be upheld.**

The increased use of the amended penal code (Sections 121, 124, and 505 (a)) and the Law Protecting the Privacy and Security of Citizens Article 8(f) to persecute human rights activists through arbitrary detention of peaceful protestors, journalists, medical professionals and other civilians opposing the coup, as well as the groundless declaration of the state of emergency, are in grave violation of international human rights laws and Myanmar's own Constitution.<sup>301</sup> Myanmar should ratify the International Covenant on Civil and Political Rights (ICCPR) and immediately uphold the principles outlined in the convention to also effectively assert the ICESCR of which Myanmar has ratified.

## **Recommendation 3: Minimizing and mitigating cyber security threats**

**3.1.** Cybersecurity should be on the minds of Myanmar IEHRDs, especially given the current shift in political climate. Open Development Myanmar has made available a poster with 9 tips for cybersecurity that can be printed out for IEHRDs.<sup>302</sup>

Front Line Defenders and Tactical Technology Collective have also developed Security in a Box toolkit with some tips and tactics for digital security. It is only available in English.<sup>303</sup> Another useful guide is available from Vice.<sup>304</sup> The following are a few other guides and tips in Burmese:

- 🔒 Risk Mitigation and Management Guide
- 🔒 Localization Lab: Burmese Surveillance Self-Defense Guides
- 🔒 MIDO: Digital Teahouse
- 🔒 Free Expression Myanmar: Protester's Toolkit

299 Article 19. 2020. Myanmar: Government's approach to 'hate speech' fundamentally flawed. Accessed May 28, 2021.

300 Minority Right Group International. 2020. Online hate speech in Myanmar: an evolving threat. Accessed May 28, 2021.

301 Thomas H. Andrews. 2021. Report of the Special Rapporteur on the situation of humanrights in Myanmar. Accessed May 24, 2021

302 The poster is available in English here and in Burmese here. It is licensed under CC BY-SA 4.0. If communities are interested in these posters please email [contact@ewmi-odi.org](mailto:contact@ewmi-odi.org).

303 See these tips and tactics here. It is licensed under CC BY-SA 3.0.

304 Access it here and here in English and here in Burmese.



### 3.2 Keep personal information private and limited to public access.

Many IEHRDs in Myanmar are not aware about using internet safely. For instance, they might show their address, family status and background information publicly, which can be misused. It is important to keep such information private and not made publicly visible, for which privacy settings should be managed while using the internet, including in social media profiles. Some applications such as Gmail and Facebook also have privacy-enhancing settings available.

### 3.3 Use a secure VPN Connection.

In order to search and click a sensitive website or news, it is important to use VPN to secure one's account or data. Many VPN are available online.

- 🔒 Use “1.1.1.1 App”. The 1.1.1.1 App adds encryption to your activities online and is usually used to help bypass internet censorship. It should be used as a basic security measure, prior to installing any VPNs. It is possible to use this app both on a smartphone as well as a computer. The application for the smartphone and computer can be downloaded from here <https://1.1.1.1/>
- 🔒 Use a VPN. All users of the internet have a unique address. A VPN masks this address so that what you do online is untraceable. A good VPN to use is Riseup. Another option is “Phiphon”, is a free and open-source VPN tool that can be used to secure your communication through online accesses. To install Phiphon VPN for your PC or smartphone, you can download from here <https://www.psiphon3.com/en/download.html>
- 🔒 In case, if one is in an unsafe situation or close to any harmful elements, turn off cell phone and take the battery out (if possible). Cell phones emit an identification number (IMSI) every few seconds to nearest cell towers. These numbers, along with SIM card numbers, are increasingly being used to identify where people are and who they are.

### 3.4 Other potential technical tools and applications are as follows:

- 🔒 Use a “burner” phone and SIM cards. This is a cheap, prepaid cell phone (not smart phone) with SIM cards that are only intended to be used for a short period of time. Pay with cash.
- 🔒 Element is now one of the most secure messaging apps.<sup>305</sup> WhatsApp, Facebook Messenger, and Viber are not secure. Signal may now also be compromised due to the need to register real world ID to cell phone data providers.
- 🔒 Decentralized web tools have long been developed but are more relevant given the current situation in Myanmar. These tools are important because they help to counter surveillance, censorship, and harassment. Decentralized web tools work by having information stored in many different places, rather than only a single location. This means that it is difficult to block access to this information. For example, Wikipedia has been blocked in Myanmar, but it has now been mirrored, decentralized, and made available here: <https://my.wikipedia-on-ipfs.org/wiki/>. The DW app (currently only made available for iOS, but soon to be made available

---

305 <https://app.element.io/>

for Android) can help individual users do this for themselves. It is available here: <https://www.dw.com/en/dw-app-defying-internet-censorship/a-52693821>

- 🔒 Documenting blocked sites is a tool for retaining the evidence of censorship.<sup>306</sup> A list of sites that are blocked in Myanmar is available here: <https://www.dw.com/en/dw-app-defying-internet-censorship/a-52693821>.
- 🔒 Tests are being conducted by Open Observatory of Network Interference, and the results can be seen here: <https://explorer.ooni.org/country/MM> Users can contribute their own tests here: <https://run.ooni.io/>, using this tool here <https://ooni.org/install/desktop>.
- 🔒 Here is an additional list of tools: <https://bubbles.sevensnails.com/>

**3.5 Other potential technical tools and applications are securely useable while internet is cut off are as follows:**

- 🔒 Mapeo is a free digital tool developed for IEHRDs to document and map information. It is offline and decentralized, which means that it is secure. Work is currently underway to localize the app for the Mekong region. More information can be found here: <https://www.digital-democracy.org/mapeo/>
- 🔒 Bridgefy is a tool that can help your apps work without the internet. More information can be found here: <https://bridgefy.me/>



Pyi Taung Su Rd, Kalaw, Myanmar

306 See more at OONI. [The Test List Methodology](#). Accessed March 9, 2021.







# THAILAND

Prepared by **Emilie Pradichit,**  
*Manushya Foundation*

# 1. Introduction

## 1.1 Profile of Indigenous Peoples in the country

### Map of distribution of ethnic groups in Thailand



There are 56 ethnic groups that continue to use traditional practices and pass on their folk wisdom from generation to generation in 67 Thai provinces - they make up nine percent of the total population of the country.<sup>307</sup> Among them, the government officially recognizes nine “hill-tribes” including the Hmong, the Karen, the Lisu, the Mien, the Akha, the Lahu, the Lua, the Thin and the Khamu,<sup>308</sup> and the tenth group Palaung sometimes is also included in some official documents.<sup>309</sup> The official number confirmed of their population is not available as there is none of the slot classified by race or made for profiling within the household survey and registration in Thailand.<sup>310</sup> It has been estimated that the Indigenous population in Thailand is around five million people, which accounts for 7.2% of the total population.<sup>311</sup>

The Indigenous Peoples (IPs) in Thailand are generally found in the highlands and/or remote forest areas, including offshore islands. They are residing mainly in three geographical regions of the country<sup>312</sup> (Please also see Figure 1):

📍 South: Indigenous fisher communities (referred to as the Chao Ley) and small populations of hunter-gatherers (Mani people);

Source: <https://img.17qq.com/images/mhhngpnppsy.jpeg>

307 Indigenous Women’s Network of Thailand (IWNT) and Manushya Foundation, *Raising Our Voices to Save Our Future*, September 2019, available at: <https://www.manushyafoundation.org/iwnt-report>

308 IWGIA, *Indigenous World 2020: Thailand*, 11 May 2020, available at: <https://www.iwgia.org/en/thailand/3610-iw-2020-thailand.html>

309 Indigenous Women’s Network of Thailand (IWNT) and Manushya Foundation, *Raising Our Voices to Save Our Future*, September 2019, available at: <https://www.manushyafoundation.org/iwnt-report>

310 IWGIA, *Synthesis Report on Marginalization of Vulnerable Indigenous People in Thailand*, 2018, available at: [https://www.iwgia.org/images/publications/new-publications/Synthesis\\_report\\_Marginalization\\_of\\_vulnerable\\_indigenous\\_peoples\\_in\\_Thailand.pdf](https://www.iwgia.org/images/publications/new-publications/Synthesis_report_Marginalization_of_vulnerable_indigenous_peoples_in_Thailand.pdf)

311 IWGIA, *Indigenous World 2020: Thailand*, 11 May 2020, available at: <https://www.iwgia.org/en/thailand/3610-iw-2020-thailand.html>

312 IWGIA, *Indigenous World 2020: Thailand*, 11 May 2020, available at: <https://www.iwgia.org/en/thailand/3610-iw-2020-thailand.html>

- North-east and east: small groups on the Korat plateau;
- North-west and north: many different highland peoples (known by the derogatory term Chao-Khao).

Most IPs live as fishermen or hunter-gatherers.<sup>313</sup> While they have been living in Thailand for generations, distinctions between different groups alongside biases often lead to marginalization and cause some of them to be stateless. Misconceptions about IPs have long influenced government policies as they are deemed drug producers and a threat to national security and the environment.<sup>314</sup> Although some positive developments have been made in recent years, such biases still act as one of the underlying reasons for the attitudes and actions of the government as well as continued challenges faced by IPs.

## 1.2 Legal framework on the rights of Indigenous Peoples

While the Thai government voted in favor of the adoption of the UN Declaration on the Rights of Indigenous Peoples (UNDRIP), it does not officially recognize Indigenous Peoples in the country but only acknowledges the existence of “ethnic groups/minorities” and “hill tribes”, without distinguishing in terms of rights and responsibilities.<sup>315</sup> The government claims that they are not considered to be Indigenous Peoples but Thais, who are able to enjoy fundamental rights and are protected by the laws of the Kingdom as any other Thai citizen<sup>316</sup> and also states that so-called “hill tribes” are “migrants, who by nature and historical background are not Indigenous to the country”.<sup>317</sup>

In addition to the lack of official recognition, the existing legal and institutional framework leads to the problems of legal status and citizenship for many IPs. Some of them have been left under statelessness or without nationality, which causes the denial of their access to all basic social services provided by the government. The statelessness is caused due to a combination of problems involving Thailand’s nationality, civil registration and immigration laws. Many upland IPs in the mountainous border regions in the North and Northwest were only directly incorporated into the central Thai state as recently as the 1980s.<sup>318</sup> When the first national census was undertaken in the 1950s, many Indigenous Peoples were neglected and undocumented as the government did not reach out to the remote areas where they lived and also because Indigenous Peoples were indifferent about participating in registration, as they were not fully informed.<sup>319</sup> Consequently, those who were not registered early were largely excluded from the earlier administrative efforts to identify, document and regulate its national population and ended up stateless.

313 IWGIA, Indigenous peoples in Thailand, available at: <https://www.iwgia.org/en/thailand>

314 IWGIA, *Indigenous peoples in Thailand*, available at: <https://www.iwgia.org/en/thailand>

315 Ian G. Baird, *Indigenous Peoples in Thailand: A contradictory interpretation*, 29 November 2019, available at: <https://theasiadialogue.com/2019/11/29/indigenous-peoples-in-thailand-a-contradictory-interpretation/>

316 Network of Indigenous Peoples of Thailand (NIPT), *Indigenous Peoples of Thailand*, 2 August 2012, available at: [http://www.sac.or.th/databases/ethnicedb/articles\\_detail.php?id=1310](http://www.sac.or.th/databases/ethnicedb/articles_detail.php?id=1310)

317 Morton, Micah F., *The Indigenous People’s Movement in Thailand Expands*, ISEAS, 16 December 2016, available at: [https://www.iseas.edu.sg/images/pdf/ISEAS\\_Perspective\\_2016\\_68.pdf](https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2016_68.pdf)

318 Morton, Micah F., *The Indigenous People’s Movement in Thailand Expands*, ISEAS, 16 December 2016, available at: [https://www.iseas.edu.sg/images/pdf/ISEAS\\_Perspective\\_2016\\_68.pdf](https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2016_68.pdf)

319 Institute on Statelessness and Inclusion, *Submission to the Human Rights Council at the 25th Session of the Universal Periodic Review: Thailand*, 21 September 2015, available at: <https://files.institutesi.org/ThailandUPR2015.pdf>



The Nationality Act<sup>320</sup> amended in 2008 grants Thai citizenship to IPs born in Thailand before 1992 and/or having parents with Thai nationality. Despite legal reforms and policy progress, the problem still remains. Some laws related to citizenship are unclear. For example, the Civil Registration Act fails to clearly define whether children born to “illegal migrants” in Thailand should be entitled to birth registration.<sup>321</sup> As a result, many were denied access to the procedure by officials.<sup>322</sup> Moreover, the implementation of laws and policies suffers from many difficulties. The application process is problematic, complicated and slow, and requires the submission of many different documents involving lengthy queue time and expensive travel to the application office.<sup>323</sup> Thus, despite the fact that IPs are recognized as Thai citizens, a number of Mani, Moken, Urak Lawoy and others have not been granted Thai citizenship yet.<sup>324</sup> It is estimated that more than one million in Thailand could be stateless with most of them being children and persons belonging to IPs in the northern and western highlands.<sup>325</sup> The lack of citizenship or legal status also results in violations of other fundamental rights and freedoms.

Legal framework related to lands and resources such as forests further limits the rights of IPs to sustain their livelihoods and live on their ancestral lands, mainly located in forests in protected areas or National Parks. These laws include Forests Act, National Parks Act, Land Code Act, National Reserved Forest Act, Wild Animal Preservation and Protection Act, Community Forest Act as well as the recent orders of the National Council for Peace and Order (NCPO) related to ending deforestation and encroachment on forest reserves.<sup>326</sup> With those laws and orders, the government effectively controls all land and natural resources classifying traditional lands and resources of IPs as state forestlands. Therefore, the IPs, who have been living for generations even before the creation of the modern State and whose livelihoods highly depend on the forests and its resources, are deprived of their rights to the lands, territories and resources. Forced evictions or relocation of IPs and local communities in the name of forest conservation or due to land grabbing caused by tourism and development projects are regularly undertaken by the government without any consultation or due compensation.<sup>327</sup>

320 Nationality Act (No.4), B.E. 2551 (2008), available at: [http://thailaws.com/law/t\\_laws/tlaw0367.pdf](http://thailaws.com/law/t_laws/tlaw0367.pdf)

321 Civil Registration Act (No.2) B.E. 2551 (2008), available at: <https://unstats.un.org/unsd/vitalstatkb/KnowledgebaseArticle50937.aspx>

322 Indigenous Women’s Network of Thailand (IWNT) and Manushya Foundation, *Raising Our Voices to Save Our Future*, September 2019, available at: <https://www.manushyafoundation.org/iwnt-report>

323 Institute on Statelessness and Inclusion, *Submission to the Human Rights Council at the 25th Session of the Universal Periodic Review: Thailand*, 21 September 2015, available at: <https://files.institutesi.org/ThailandUPR2015.pdf>

324 IWGIA, *Synthesis Report on Marginalization of Vulnerable Indigenous People in Thailand*, 2018, available at: [https://www.iwgia.org/images/publications/new-publications/Synthesis\\_report\\_Marginalization\\_of\\_vulnerable\\_indigenous\\_peoples\\_in\\_Thailand.pdf](https://www.iwgia.org/images/publications/new-publications/Synthesis_report_Marginalization_of_vulnerable_indigenous_peoples_in_Thailand.pdf)

325 Indigenous Women’s Network of Thailand (IWNT) and Manushya Foundation, *Raising Our Voices to Save Our Future*, September 2019, available at: <https://www.manushyafoundation.org/iwnt-report>

326 Manushya Foundation and Thai BHR Network, *The Rights of Indigenous Peoples in Business Contexts in Thailand*, March 2019, available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_1925e7781afc4f50831a1c5e77ebb404.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_1925e7781afc4f50831a1c5e77ebb404.pdf)

327 Indigenous Women’s Network of Thailand (IWNT) and Manushya Foundation, *Raising Our Voices to Save Our Future*, September 2019, available at: <https://www.manushyafoundation.org/iwnt-report>

### 1.3 The situation of Indigenous Environmental Human Rights Defenders (IEHRDs)

As the legal and institutional framework is generally not favourable for the rights of Indigenous communities, IPs and activists in Thailand are continuously struggling for land and Indigenous rights. The indigenous movement in Thailand officially came into being in August 2007 when a coalition of ethnic groups established Network of Indigenous Peoples of Thailand to campaign for legal recognition of IPs and their rights through various strategies including public demonstrations, independent media productions and bureaucratic lobbying.<sup>328</sup> In addition, there are several Indigenous-led non-governmental organizations (NGOs) such as Inter-Mountain Peoples Education and Culture in Thailand Association and Indigenous Women Network of Thailand. Grassroots organizations, community members and individual activists also make a vital contribution to the advancement of Indigenous rights.

However, in recent years, shrinking civic space and growing threats to Indigenous activists have become an increasing concern. After the 2014 coup, the NCPO has enacted restrictive laws, resulting in a challenging climate for human rights defenders (HRDs). Regardless of the fact that NCPO no longer exists and in 2019 elections were held, the military-affiliated government has shown no signs of relaxing restrictions on freedoms of expression, assembly, privacy, independent press and access to information. The State has repeatedly used judicial harassment to target HRDs. Surveillance, intimidation, threats and even physical assaults, arbitrary detention and extrajudicial killings of HRDs have been reported.<sup>329</sup> IEHRDs are increasingly at risk of violence, discrimination, and other violations of their human rights as they engage in protests and expression of concerns over negative impacts of business operations, which means that they face reprisals not only from the authorities but also from the private sector.

As new technologies develop and become more common, activists who look to come together to advance democracy, peace and development increasingly turn to online spaces. Social media and instant messaging apps have become prominent tools for social movements. There are more than 52 million active social media users out of a total population of 67 million people with 17 million Thai Twitter accounts. Millions of netizens have used online hashtags such as #WhyDoWeNeedAKing, #GetOutPrayuth, and #SaveAnonymous to voice their anger, opinions, and views over recent incidents and demand basic rights.<sup>330</sup> Meanwhile, the government has moved forward to crack down on online movement through a series of legislation and policies, empowering government agencies to restrict access to websites, monitor online communications, criminalize online speech, censor online content and collect user data. In this constrained atmosphere, IEHRDs encounter a lot of challenges for undertaking human rights related activities online.

328 Morton, Micah F., *The Indigenous People's Movement in Thailand Expands*, ISEAS, 16 December 2016, available at: [https://www.iseas.edu.sg/images/pdf/ISEAS\\_Perspective\\_2016\\_68.pdf](https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2016_68.pdf)

329 Front Line Defenders, *#Thailand*, available at: <https://www.frontlinedefenders.org/en/location/thailand>

330 Australian Strategic Policy Institute, *Thailand's hashtag activism targets political change*, 20 April 2020, available at: <https://www.aspistrategist.org.au/thailands-hashtag-activism-targets-political-change/>

## 2. Methodology

The methodologies used for this report include desk research, interviews and consultations with IEHRDs at local and national levels. Primary sources including voices, concerns, cases and experiences of IEHRDs were collected directly from the activities of Asia Indigenous Peoples Pact (AIPP) and Manushya Foundation. For example, AIPP organized a regional exchange and training on digital security from 30 September to 2 October 2020, where Indigenous human rights activists from 10 countries participated and shared their experiences with online interferences, including threats, prosecution, hacking and internet shutdown in relation to their works on Indigenous rights. AIPP carried out analysis of current challenges while Manushya Foundation supported AIPP to assess legal framework and propose recommendations for IEHRDs, and also engaged with local Indigenous communities to gain insights and identify human rights violations.

This report is also based on desk-research, including a systematic literature review of relevant laws and government regulations; reports and observations/recommendations of United Nations (UN) human rights bodies and NGOs; online news articles; expert papers and other publications. It aims to present an analysis of the legal framework on cybersecurity laws and potential impacts on IEHRDs.



Thailand Indigenous Peoples marching for the recognition of their rights during the International Day of the World's Indigenous Peoples, Chiang Mai, Thailand.

### 3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age

#### 3.1 Constitutional provisions and laws stipulating the rights of IEHRDs

**HUMAN DEVELOPMENT INDEX (HDI):** 0.777 (2019)  
**NUMBER OF INTERNET USERS IN THAILAND:** 48.59 million (as of January 2021)  
**LEVEL OF FREEDOM:** 30/100 (with 0 being least free and 100 being most free, Freedom in the World 2021 – Freedom House)  
**LEVEL OF PRESS FREEDOM:** Ranked 137<sup>th</sup> out of 180 countries (with 1<sup>st</sup> being highest level of press freedom, World Press Freedom Index 2021 - Reporters Without Borders)  
**LEVEL OF FREEDOM ON THE NET:** 35/100 (with 0 being least free and 100 being most free, Freedom on the Net 2020 – Freedom House)  
**GLOBAL CYBERSECURITY COMMITMENT:** Ranked 44<sup>th</sup> out of 182 countries with a score of 86.5/100 (with 1<sup>st</sup> being highest and 182<sup>nd</sup> being the lowest commitment – ITU Global Cyber Security Index)

Thailand's 2017 Constitution guarantees the rights and liberties of Thai people.<sup>331</sup> It stipulates freedom of expression and liberty of communication in Articles 34 and 36 but restriction can be imposed for the purpose of maintaining the State's security, protecting the rights or liberties of other persons, maintaining public order or good morals or protecting people's health. With regards to online privacy, the Constitution provides, in Article 32, that everyone shall have the right to privacy, dignity, and reputation, and that abuse of personal information shall not be permitted unless provided by law

and necessary for the public interest. Freedom of media is guaranteed under Article 35 of the Constitution that prohibits censorship of any news or statements prior to publication in a newspaper or any media unless the State is at war. Article 44 of the Constitution upholds the freedom of any person to assemble peacefully, which can be restricted for maintaining security of the State, public safety, public order or good morals, or for protecting the rights or liberties of other persons. Article 41 of the Constitution recognizes the right of people to present a petition to a State agency and be informed of the result of its consideration in due time.

The 2017 Constitution also acknowledges the rights of a person and community to access public data or information and participation in decision-making affecting them. Article 41 of the Constitution states that a person and community have the right to "be informed and have access to public data or information in possession of a State agency as provided by law". Further, Article 59 provides that "the State shall disclose any public data or information in its possession, not related to the security of the State or government confidentiality and shall ensure that the public can conveniently access such data or information". Moreover, Article 78 of the Constitution also provides for the participation of people and communities

331 Thailand's Constitution of 2017, available at: [https://www.constituteproject.org/constitution/Thailand\\_2017.pdf](https://www.constituteproject.org/constitution/Thailand_2017.pdf)

“in various aspects of the development of the country, in the provision of public services at both national and local levels, in the scrutiny of the exercise of State power, in combating against dishonest acts and wrongful conducts, as well as in decision making in politics and in all other matters that may affect them”.

Beyond the Constitution’s provisions, Article 48 of the Enhancement and Conservation of the National Environmental Quality Act 1992<sup>332</sup> provides that the development of Environmental Impact Assessment (EIA) for development projects should include an assessment of the impact on health. The Act also lays out the foundation for public participation in the development of environmentally harmful projects.

Despite the explicit constitutional and legal provisions in Thailand, challenges remain in peacefully exercising the rights to assembly, expression, privacy and access to information, and ensuring the participation for IPs and IEHRDs affected by development projects and business conduct. Some restrictive laws fall short of international standards for the rights of IPs and IEHRDs.

## 3.2 Legal framework restricting offline activities of HRDs

### 3.2.1 Criminal Code<sup>333</sup>

Article 112 on *lèse-majesté*, Article 116 on sedition, and Articles 326 to 333 on slander and libel of the Criminal Code include vague and broadly formulated crime of defamation, which has routinely been invoked to restrict freedom of expression and target those reporting on human rights abuses committed by government officials and private corporations. Article 112, often referred to as Thailand’s *lèse-majesté* law, provides a penalty of up to 15 years imprisonment for anyone who defames, insults or threatens the King, the Queen, the Heir-apparent, or the Regent”. Although this law has been used less frequently in recent years, critics of monarchy continue to face prison under other laws.<sup>334</sup> Article 116 provides a penalty of up to seven years in prison for anyone, who uses words or writings to

- (1) bring about a change in the laws of the country or the government by the use of force or violence;
- (2) raise unrest and disaffection among the people in a manner likely to cause disturbance in the country; or
- (3) cause the people to transgress the laws of the country.

Article 326 states that “whoever imputes anything to the other person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to be hated or scorned, is said to commit defamation and shall be punished with imprisonment not exceeding one year or fined not exceeding twenty thousand baht, or both.”

332 Enhancement and Conservation of the National Environmental Quality Act, B.E. 2535 (1992), available at: [http://web.krisdika.go.th/data//document/ext809/809866\\_0001.pdf](http://web.krisdika.go.th/data//document/ext809/809866_0001.pdf)

333 Penal Code B.E. 2499 (1956), available at: <http://un-act.org/wp-content/uploads/2015/11/Criminal-Code-B.E.-2499-1956.pdf>

334 Prachatai, *PM says royal mercy stopped use of lèse majesté law*, 16 June 2020, available at: <https://prachatai.com/english/node/8592>; The Reuters, *Explainer: Thailand’s lese majeste law*, 4 August 2020, available at: <https://www.reuters.com/article/us-thailand-protests-monarchy-explainer-idUSKCN2501Q1>

Under Article 328, if the defamation is committed by means of a document, video, drawing, or any other means, it is punishable by up to two years in prison.

### **Weaponization of criminal defamation against both online and offline speech**

The vague and broadly formulated offenses of defamation are regularly invoked to target individuals not only for making statements offline but also for publishing content on the internet. In the case of two IEHRDs and six Karen community members from Omkoi District, Chiang Mai Province, the local mining company sued them for defamation under the Criminal Code as they read out a statement and made a speech against the coal mine in a protest on 5 June 2019.<sup>335</sup> A large number of activists, who post online content critical of government policy or development projects, frequently face defamation charges. While the UN has been repeatedly calling on the Thai government to decriminalize defamation and stop silencing HRDs,<sup>336</sup> such provisions of the Criminal Code that contravene international law and standards still exist.

### **3.2.2 The 2015 Public Assembly Act<sup>337</sup>**

Enacted in 2015, the Public Assembly Act gives authorities sweeping powers to ban public assemblies on vague and arbitrary grounds. Under Article 10, it requires anyone seeking to hold a public assembly to notify the authorities at least 24 hours in advance of the date, time, place, and aim of the assembly. Failure to provide such notice is an offense with a possible penalty of up to 10,000 baht as per Article 28. Such requirement does not meet international laws, which provide that prior notification can be applied as a procedure to allow the authorities to promote the exercise of the right of peaceful assembly but should not be needed for authorization.<sup>338</sup> Moreover, the Act also contains vague provisions in relation to applicable restrictions, including that a public assembly may be restricted if such actions may cause disruption and public disorder. It prohibits public assembly near or in the locations such as royal palaces and residences, the National Assembly, Government House, and the Thai courts under Article 7. Under Article 8, public assembly is also prohibited to obstruct State agencies, airport or public transport, hospitals, education or religious establishment, foreign embassies or consulates or other international organization, or other places notified by the government. Further, the authorities are allowed to instruct the organizers to modify the gathering or prohibit the assembly if it deems the public assembly breaches Articles 8, 9 or 10.

Most problematically, the law imposes criminal penalties, for example under Articles 15 and 16, for vaguely worded “duties” of both organizers and participants of public assembly, including a duty not to cause “unreasonable inconvenience” to any person. Violation of duties can be punished with a fine of up to 10,000 baht or be liable to imprisonment, which is in

335 IPHRDs-Thailand, *SLAPP Against IPHRDs at Omkoi District*, 8 April 2020, available at: [https://tlhr2014.com/archives/14207](http://www.eihrdthailand.net/blog/news/รายงานสถานการณ์ละเมิดส/ ; TLHR, จากขบวนคัดค้านเหมืองแร่ทองคำสู่การถูกฟ้องคดีปิดปากของแกนนำชาวบ้าน</a>, 25 October 2019, available at: <a href=)

336 OHCHR, *Thailand: UN experts condemn use of defamation laws to silence human rights defender Andy Hall*, 17 May 2018, available at: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23095&LangID=E>

337 Public Assembly Act, B.E. 2558 (2015), available at: <http://lawdrafter.blogspot.com/2015/08/translation-thai-public-assembly-act-of.html>

338 OHCHR, *Joint Letter from 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; and the Special Rapporteur on the situation of human rights defenders to the Thai government*, THA 12/2014, 11 November 2014, available at: <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=21921>



conflict with international law. Consequently, this Act has been routinely used to hamper freedom of assembly and to harass the people involved, which has had a chilling effect on IPs and IEHRDs wishing to protest against land grabbing and forced relocation.

### 3.2.3 Broadcasting Act and Media Law

The Thai government monitors media content from all media sources under laws curtailing freedom of press.<sup>339</sup> Broadcasting and Television Business Act empowers the National Broadcasting and Telecommunications Commission (NBTC) to suspend or revoke the licenses of radio or television operators broadcasting content deemed false, defamatory to the monarchy, harmful to national security or critical of the government.<sup>340</sup> A draft Bill on the Promotion of Media Ethics and Professional Standards raises further concerns over media independence as it would create a national professional media council mandated to issue codes of conduct to journalists and media outlets, rule on complaints and impose fines of at least 1,000 baht per day on a legal media entity or at least 100 baht per day on a journalist.<sup>341</sup> As a result, press and media often lean toward self-censorship, thereby deterring IPs and IEHRDs from advocating through traditional media and accessing uncensored information.

### 3.2.4 Emergency Decree

In March 2020, the Thai government invoked the Emergency Decree on Public Administration in Emergency Situation, B.E. 2548 (2005) to declare a state of emergency and implement a set of regulations aimed at combatting the spread of COVID-19.<sup>342</sup> The Decree has been extended several times and is now set to last until 28 February 2021.<sup>343</sup> It bans public gatherings, stating that “it is prohibited to assemble, to carry out activities, or to gather at any place that is crowded, or to commit any act which may cause unrest”. Violations can be punishable by up to two years’ imprisonment.<sup>344</sup> Under the Decree, by October 2020, more than 80 protesters<sup>345</sup> faced charges for participating in youth-led demonstrations, which started in August that year demanding a new constitution, reforms of the monarchy and resignation of the Prime Minister. It has also been invoked to impose broad censorship to impede freedom of expression and media both online and offline as it prohibits the sharing

339 U.S. State Department, *Thailand 2019 Human Rights Report*, 2019, available at: <https://www.state.gov/wp-content/uploads/2020/02/THAILAND-2019-HUMAN-RIGHTS-REPORT.pdf>

340 Broadcasting and Television Business Act B.E.2551 (2008), available at: [http://web.krisdika.go.th/data/outsite/outsite21/file/Broadcasting\\_and\\_Television\\_Businesses\\_Act\\_BE\\_2551\\_\(2008\).pdf](http://web.krisdika.go.th/data/outsite/outsite21/file/Broadcasting_and_Television_Businesses_Act_BE_2551_(2008).pdf)

341 Freedom House, *Freedom on the Net: Thailand 2020*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020>

342 Prachatai, *Thailand: Stop using emergency powers to restrict the rights of protesters*, 30 June 2020, available at: <https://prachatai.com/english/node/8619>; The Reuters, Thai emergency decree extended to end-November to curb coronavirus, 28 October 2020, available at: <https://www.reuters.com/article/us-health-coronavirus-thailand-idUSKBN27D0VM>

343 The Government Public Relations Department, *Emergency Situation Declaration to Be Extended Until the End of February*, 5 January 2021, available at: [https://thailand.prd.go.th/ewt\\_news.php?nid=10593&filename=index](https://thailand.prd.go.th/ewt_news.php?nid=10593&filename=index)

344 Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFEnet), *Joint Solidarity Statement – Thailand: Stop Digital Dictatorship over Online Freedom*, 25 October 2020, available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_a6ec0138949847db996260c8308b0c0b.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_a6ec0138949847db996260c8308b0c0b.pdf); Prachatai, *Thailand: Stop using emergency powers to restrict the rights of protesters*, 30 June 2020, available at: <https://prachatai.com/english/node/8619>

345 Fortify Rights, *Thailand: Protect Protest Rights, Drop Charges Against Activists*, 23 October 2020, available at: <https://www.fortifyrights.org/tha-inv-2020-10-23/>; Human Rights Watch, *Thailand: Emergency Decree Pretext for Crackdown*, 15 October 2020, available at: <https://www.hrw.org/news/2020/10/15/thailand-emergency-decree-pretext-crackdown>

of news that is “false or may instigate fear among the people”.<sup>346</sup> An Indigenous woman HRD has revealed her concerns over the Decree in April as the restrictions hinder HRDs from carrying out their activities.<sup>347</sup>

### 3.3 Cybersecurity laws and policies restricting online activities of IEHRDs

#### 3.3.1 Computer Crime Act (CCA) 2007 (amended in 2017)<sup>348</sup>

The CCA (officially known as Commission of Computer-related Offences Act) provides the Thai government with unlimited power to restrict online speech, undertake surveillance and warrantless searches of personal information and data, undermine the right to use encryption and anonymity, and force service providers to facilitate government surveillance and censorship. It contains overly broad provisions that have been frequently invoked to violate the right to freedom of speech. Section 14 (1), (2) and (3) of the law provides for a sentence of up to five years in prison and a fine of up to 100,000 baht for various offences, including “bringing into a computer system a computer data which is distorted or fake” in a manner to cause damage “to the public”, “the maintenance of national security, public security, national economic security or an infrastructure involving national public interest”, or “which constitutes an offence relating to security of the Kingdom or an offence relating to terrorism under the Penal Code”. Subsection 14 (5) criminalizes the mere dissemination of data under 14 (1), (2), (3) or (4).

The above legal provisions are excessively broad and fail to meet international standards. Under international law, restrictions on speech must be necessary only to protect the rights or reputation of others, national security or public order or public health or morals and conform to the strict test of necessity and proportionality.<sup>349</sup> Restricting speech on grounds of the likelihood of “damage to the public”, which lacks specific definition in the law is unjustified. The very vagueness of the phrase opens to interpretation, resulting in the potential of misuse by government officials to target anyone, who criticizes the government. Similarly, although protecting public order is a legitimate basis for restricting speech under international law, the Act fails to narrowly draw such terms to impose restrictions as little as possible.

346 Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFEnet), *Joint Solidarity Statement – Thailand: Stop Digital Dictatorship over Online Freedom*, 25 October 2020, available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_a6ec0138949847db996260c8308b0c0b.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_a6ec0138949847db996260c8308b0c0b.pdf); Prachatai, *Thailand: Stop using emergency powers to restrict the rights of protesters*, 30 June 2020, available at: <https://prachatai.com/english/node/8619>

347 Protection International, *The right to defend under COVID-19: The voice of a Thai Woman Human Rights Defender*, 8 April 2020, available at: <https://www.protectioninternational.org/en/news/right-defend-under-covid19-voice-thai-woman-human-rights-defender>

348 Computer Crime Act 2007, available at: <https://www.samuihorsale.com/law-texts/computer-crime-act.html>; Computer Crime Act B.E. 2560 (2017), available at: [http://web.krisdika.go.th/data//document/ext809/809777\\_0001.pdf](http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf)

349 UN Human Rights Committee, *General Comment No. 34*, UN Doc. CCPR/C/GC/34 (2011), para. 22, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/453/31/PDF/G1145331.pdf?OpenElement>; International Covenant on Civil and Political Rights (1976), available at: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

The CCA also provides for obligations of Internet Service Providers (ISPs). Section 15 of the Act imposes criminal liability on an ISP for content without requiring intent on the part of the ISP, which creates a strong incentive to censor. As a result, intermediaries block or take down material that they fear may be found to be in violation of the law. Section 26 problematically requires ISPs to retain user data for 90 days or allow for warrantless access to user communication. Furthermore, a criminal defamation provision still exists as Section 16 continues to criminalize the use of images of another person that have been created, edited, or adapted in a way that “is likely to impair the reputation of such other person or to expose such other person to hatred or contempt”, which the UN has repeatedly urged the Thai government to abolish.<sup>350</sup>

### 3.3.2 2019 Cybersecurity Act<sup>351</sup>

The Cybersecurity Act toughens online monitoring and grants authorities the power to carry out mass surveillance. Under Section 3, “maintaining cybersecurity” is defined as any measure to mitigate the risk of cyber threats that “affect national security, economic security, martial security, and public order in the country” rather than to protect the security of individuals and netizens and to cope with threats posed in the digital space. It fails to clearly define those elements and how far the limits will be applied and used. The broad linkage made between cybersecurity and national security, public order, economic security and public interest will allow for interpretations that could lead to misuse and the violation of human rights of individuals.

The Act allows government bodies and agencies to collect personal information when there is a deemed cybersecurity risk. Those include National Cybersecurity Committee (NCSC), Cybersecurity Regulation Committee (CRC), Office of the National Cybersecurity Committee, and Committee Managing the Office of the National Cybersecurity Committee (CMO). Court permission and oversight is only permitted for non-critical and critical level cybersecurity incidents, with the Act providing for reporting to the Court after a crisis level cybersecurity incident has already been addressed. In the absence of any independent monitoring of the power exercised by the government authorities under this Act, officials are given very broad power, which could result in serious privacy breaches and the crackdown on online activities of HRDs.

Private enterprises have reporting obligations with respect to cybersecurity incidents and failure to report or submit risk assessment reports could be subjected to imprisonment and heavy penalty, according to Sections 73 and 74 of the Act. In this case, the private sector such as information technology and telecommunications companies could compromise the privacy and human rights of individuals if asked to, which violates UN Guiding Principles on Business and Human Rights (UNGPs).

### 3.3.3 Personal Data Protection Act (PDPA)<sup>352</sup>

350 OHCHR, *Thailand: UN experts condemn use of defamation laws to silence human rights defender Andy Hall*, 17 May 2018, available at: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23095&LangID=E>

351 Cybersecurity Act, B.E. 2562 (2019), available at: <https://cyrilla.org/en/entity/4nywjpircms?file=1588770279351q8g2xeaybw.pdf&page=1>

352 Personal Data Protection Act, B.E. 2562 (2019), available at: <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf>

The PDPA provides protection for personal data by restricting the collection, use, disclosure or tampering of personal data without the consent of its owner, and outlining how businesses can collect, use, or disclose personal information. The Act contains many progressive provisions, including obtaining consent specifically from the subject, whose information is being collected, prior to or at the time of collection - either in writing or through electronic means. In addition, the collection of data must be for a lawful purpose and be of direct relevance or necessary for the activities of the data controller. Unfortunately, the positive provisions of the Act are yet to be implemented as the authorities have delayed the implementation of the Act that should have taken effect in April 2020, thus failing to ensure the safety of personal data.<sup>353</sup>

Meanwhile, the Act itself has problematic provisions as it also sets exemptions, allowing Parliament and any committee appointed by them as well as the authorities to collect and use data “to maintain state security, including financial security of the state or public safety” and “with respect to the prevention and suppression of money laundering, forensic science or cybersecurity” under Section 4. Those exceptions remain open to interpretation with no explanation provided on how government operations that violate data privacy are addressed.

### 3.3.4 National Intelligence Act<sup>354</sup>

The 2019 National Intelligence Act, which went into effect in April 2019, gives the National Intelligence Agency unrestricted power to obtain any information from government agencies or individuals in the case of “national security”, a term that remains undefined. It also allows the Agency to force ISPs to hand over information, including sensitive personal data, whenever it requests. In the situation when the information is not provided by a government agency or individual, the Agency has authority to “use any means, including electronic, telecommunication devices or other technologies” to obtain it.

### 3.3.5 Agencies and policies

The CRC, established under the Cybersecurity Act, plays a key role in the implementation of the Act and is given broad powers to conduct surveillance and respond to cybersecurity incidents without any explanation on substantive or procedural checks and balances to protect individual rights. Additional bodies such as the NCSC, the Office of the National Cybersecurity Committee, and the CMO have also been operationalized under the CCA and the PDPA.<sup>355</sup>

The National Legislative Assembly (NLA) has established the Ministry of Digital Economy and Society (MDES) in 2016, which is in charge of implementing policy and enforcing

353 Civil Rights Defenders, *Thailand's Facial Recognition policy in the Deep South raises serious human rights concerns*, 18 June 2020, available at: <https://crd.org/2020/06/18/thailands-facial-recognition-policy-in-the-deep-south-raises-serious-human-rights-concerns/?fbclid=IwAR1Iz5MOg6bSJWNZDpgHFophWOvujhVejzibGTUEkS SpulAgZ8o7srKSE3c> ; Global Compliance News, *Thailand: Postponement of Thailand's Personal Data Protection Act*, 13 June 2020, available at: <https://globalcompliancencnews.com/thailand-postponement-of-thailands-personal-data-protection-act-01062020/>

354 National Intelligence Act, B.E. 2562, available at: <https://www.nia.go.th/FILEROOM/CABFRM01/DRAWER01/GENERAL/DATA0041/00041619.PDF>

355 Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, September 2019, available at: <https://www.manushyafoundation.org/study-on-cybersecurity-act>

the CCA.<sup>356</sup> In October 2019, it ordered coffee shops, restaurants, and other venues that offer public Wi-Fi to retain the data of users, including names, browsing history, and log files, for at least 90 days.<sup>357</sup> The Anti-Fake News Center, established by the MDES in November 2019 is mandated to combat false and misleading information that violates the CCA, particularly Sections 14(2) and 14(3)<sup>358</sup> of the Act, and issue “corrections” through its website, social media accounts and news outlets.<sup>359</sup> It deals with four main categories of false information: disasters; economic, banking and equity issues; health issues and illegal health products and services; and news and information with national security, social and moral risks.<sup>360</sup> In May 2020, a new cyber police unit with 1,700 officers was approved to monitor for cybercrimes, including those related to “fake news”.<sup>361</sup>



The banner with message “In solidarity of Indigenous Peoples in Asia” for Karen people in Bangkloi village, Thailand.

- 356 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020>
- 357 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020> ; VOA, *Thailand's Coffee shops told to track, save public Wi-Fi traffic*, 10 October 2019, available at: <https://www.voanews.com/east-asia-pacific/thailands-coffee-shops-told-track-save-public-wi-fi-traffic>
- 358 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020> ; Channel News Asia, *Thailand launches anti-fake news centre*, 3 November 2019, available at: <https://www.channelnewsasia.com/news/asia/thailand-launches-anti-fake-news-centre-video-12057282>
- 359 U.S. State Department, *Thailand 2019 Human Rights Report*, 2019, available at: <https://www.state.gov/wp-content/uploads/2020/02/THAILAND-2019-HUMAN-RIGHTS-REPORT.pdf> ; Reuters, *Thailand unveils 'anti-fake news' center to police the internet*, 1 November 2019, available at: <https://www.reuters.com/article/us-thailand-fakenews/thailand-unveils-anti-fake-news-center-to-police-the-internet-idUSKBN1XB48O>
- 360 U.S. State Department, *Thailand 2019 Human Rights Report*, 2019, available at: <https://www.state.gov/wp-content/uploads/2020/02/THAILAND-2019-HUMAN-RIGHTS-REPORT.pdf>
- 361 Bangkok Post, *Cyber cops unit to be set up*, 12 June 2020, available at: <https://www.bangkokpost.com/thailand/general/1933404/cyber-cops-unit-to-be-set-up> ; VietNamNet, *Thailand to set up cyber police bureau*, 14 June 2020, available at: <https://vietnamnet.vn/en/sci-tech-environment/thailand-to-set-up-cyber-police-bureau-648750.html>



## 4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases

### 4.1 Strategic lawsuit against public participation (SLAPP), threats and harassment for online activity

IPs and IEHRDs who express dissenting views online have faced harassment, intimidation, arrest and prosecution by the authorities under the Computer Crime Act (CCA) and the Criminal Code. As the CCA retains the problematic terms such as “false” and “distorted” computer information, the incorrect interpretation of the law persists. Violation of the law can lead to a maximum five-year prison sentence. The positive progress made by the judiciary is that a large number of cases falsely initiated against HRDs have been dismissed.<sup>362</sup> Apart from judicial harassment, the authorities also apply extra-legal means to intimidate activists and shrink civic space. The common practices include arbitrary detention, visits at home, involuntary collection of personal data and forced signature in memorandum of understandings (MOUs) or other documents restricting similar future behavior. These methods are used without prior notification of individuals’ rights.<sup>363</sup> Another harmful practice is state-sponsored disinformation and online hate speech and harassment against disadvantaged groups and activists. The Internal Security Operations Command has been carrying out Information Operations (IOs) to conduct cyber warfare against activists, politicians and academics, who promote democracy, peace and human rights, by funding military-linked accounts publishing posts, stories and articles critical of them, as well as manipulating information and disseminating hate speech. In this manner, the legitimacy and reputation of the civil society organizations, activists, and IPs organizing protests against the government can be defamed, disqualified and destroyed by IOs.<sup>364</sup> Thus, the risk of criminal charges, lengthy legal processes and targeted harassment or violence have discouraged IEHRDs from exercising their right to freedom of expression in practice.

#### Case of woman EIHRD, who was visited by the police<sup>365</sup>

On 9 May 2020, Katima Leeja, a 35-year-old Indigenous Lisu woman human rights defender from Chiang Dao District, Chiang Mai Province, was visited by a military officer in

362 Manushya Foundation and Thai Business & Human Rights Network, *The Protection of Human Rights Defenders*, 2019, available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_6d64d56d0f7c478298e000b18aed6f81.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_6d64d56d0f7c478298e000b18aed6f81.pdf)

363 Civil Rights Defenders, *Thailand’s Facial Recognition policy in the Deep South raises serious human rights concerns*, 18 June 2020, available at: <https://crd.org/2020/06/18/thailands-facial-recognition-policy-in-the-deep-south-raises-serious-human-rights-concerns/?fbclid=IwAR1Iz5MOg6bSJWNZDpgHFophWOvuJhVejzibGTUEkSSpulAgZ8o7srKSE3c>; Prachatai, *PM says royal mercy stopped use of lèse majesté law*, 16 June 2020, available at: <https://prachatai.com/english/node/8592>

364 Australian Institute of International Affairs, *Are The Thai Army’s Information Operations Self-Defeating?*, available at: <https://www.internationalaffairs.org.au/australianoutlook/are-the-thai-armys-information-operations-self-defeating/>; Bangkok Post, *Isoc says ‘cyber war’ only on fake news*, 28 February 2020, available at: <https://www.bangkokpost.com/thailand/general/1867154/isoc-says-cyber-war-only-on-fake-news>

365 Prachatai English, *Indigenous woman human rights defender visited by military officer after protest against the alleged violence by forest authorities*, 12 May 2020, available at: <https://prachatai.com/english/node/8510>



plain clothes after she uploaded a video on Facebook on May 5 criticizing the use of violence by the authority during a land dispute incident and demanding investigation. The police asked about her involvement in land rights and IPs rights activities as well as personal information including her birthday, marital status, phone number, members residing in the house, her parents and siblings' names, and their occupations. After this visit, she and her families were worried about her safety.

#### **Case of Wuth Boonlert, who was charged for a Facebook post**

Wuth Boonlert is an Indigenous Karen community leader who has advocated community and Indigenous rights of the Karen people in Tanaosri region and Kaeng Krachan National Park. In 2016, Wuth shared a post written by a retired national park employee Samak Donnapee, in which he criticized some government officials who have trespassed into a preserved forest area to construct "Chairatchapleuk Resort". This case was brought to the court by both the public prosecutor's office and a public official under Article 329 of the Criminal Code and underwent a long legal process. On 18 November 2019, the Minburi Criminal Court found both him and Samak Donnapee not guilty and dismissed the case, noting that his sharing of the post constitutes posts for the purposes of only examining the work of government officials and carry insufficient weight to cause damage to the joint plaintiffs.<sup>366</sup> On 24 November 2020, the Court of Appeals also dismissed the case against Wuth, ruling that the post of Samak Donnapee constitutes a criticism of the officers in charge with fairness as an honest expression of the feelings of the general public in accordance with Section 329(3) of the Criminal Code.<sup>367</sup>

#### **Case of hate speech and online harassment by IOs related to Facebook posts**

On 25 January 2020, a Facebook post was made of the wife of EIHRD Porla-jee "Billy" Rakchongcharoen, who was murdered in Kaeng Krachan National Park (KKNP) where the Karen community has resided sustainably for hundreds of years but faced violent eviction. Billy's wife has expressed her discontent with the fact that Billy's case has yet to be solved while the KKNP has become a UNESCO World Heritage. This post has been filled with a large number of negative comments from IOs accounts that denounced Billy's case has yet to be solved the Karen IPs.<sup>368</sup> Another example can be seen in a Facebook post containing a video of the protest by Karen IPs in KKNP that took place on 15 February 2021 in front of the UN in Bangkok. Comments from IOs accounts stigmatized Karen IPs and IEHRDs by referring to them as "aliens from Burma", "Thai person with a Burmese heart" and those who organized rallies to "earn money".<sup>369</sup>

366 The Minburi Criminal Court, *Court Judgement*, 18 November 2019, available at: [https://cfj.org/wp-content/uploads/2020/07/Judgement\\_Government-of-Thailand-and-Chaiway-Limlikhitaksorn-v.-Woth-Boonlert-and-Samak-Donnapee.pdf](https://cfj.org/wp-content/uploads/2020/07/Judgement_Government-of-Thailand-and-Chaiway-Limlikhitaksorn-v.-Woth-Boonlert-and-Samak-Donnapee.pdf); Voice from Thais, *Fact Sheet on the criminal defamation lawsuit against Mr. Wut Boonlert*, available at: [https://voicefromthais.files.wordpress.com/2019/09/fact-sheet\\_wut-boonlert\\_-en\\_edited\\_g.pdf](https://voicefromthais.files.wordpress.com/2019/09/fact-sheet_wut-boonlert_-en_edited_g.pdf); The Columbia Law School Human Rights Institute, *Government of Thailand & Chaiwat Limlikhitaksorn v. Wuth Boonlert & Samak Donnapee*, July 2020, available at: <https://cfj.org/wp-content/uploads/2020/07/Fairness-Report-on-the-Trials-of-Wut-Boonlert-and-Samak-Donnapee-in-Thailand.pdf>

367 Prachatai, ศาลอุทธรณ์ยกฟ้องคดีที่ 'ชัยวัฒน์ ลิมลิกhitอักษร' ฟ้องหมิ่นฯ นักสิทธิ, 23 December 2020, available at: <https://prachatai.com/journal/2020/12/90940>

368 คมชัดลึก, Facebook post, 25 January 2020, available at: <https://www.facebook.com/komchadluek/posts/10158258701529668> ;

369 The Reporters, Facebook post, 9 February 2021, available at: <https://www.facebook.com/TheReportersTH/videos/888345671952642>

## 4.2 Judicial harassment and defamation charges initiated by businesses

In addition to government authorities, private companies also file defamation cases under the Criminal Code and the CCA against HRDs, activists, and individuals for online activities. Defamation charges have frequently targeted EHRDs when they oppose development projects or forced eviction that cause the loss of livelihoods of local communities. An analysis of the situation of EHRDs by the UN Special Rapporteur on the situation of HRDs in 2016 indicated that Thailand is one of the ten most dangerous countries for EHRDs.<sup>370</sup> Particularly, IEHRDs are more vulnerable since they belong to groups that are marginalized in society and face intersectional discrimination.

### Case of Omkoi mining company against four students<sup>371</sup>

In 2019, four students from Maejo University went to Omkoi District, Chiang Mai Province to collect data regarding the impact of coal mining on the local Karen community. Afterwards, they published their studies on Prachatai online website, exposing that the community members were manipulated into selling their land to the company without knowing what their land would be used for and were threatened to stay silent. Although the findings published did not explicitly state any company's name, the mining company 99 Tuwanon Co. Ltd. filed defamation charges against the four students under Section 328 of the Criminal Code. Omkoi Provincial Police Station issued warrants in November 2019.

## 4.3 Limited access to information by blocking and removal of content online

The Thai government excessively controls critical content online by blocking webpages and virtual private networks (VPNs) and requiring major companies such as Google, Twitter and Facebook to remove content from their platforms on the basis of the Cybersecurity Act and CCA. Blocking of the online content deemed critical of the monarchy and the government on grounds of national security is widespread whereas the extent of this method remains unclear due to a lack of transparency.<sup>372</sup> In October 2020, the MDES ordered to suspend many online media outlets, including Voice TV, Prachatai, The Reporters, and The Standard citing the CCA and the Emergency Decree,<sup>373</sup> but the court afterwards has lifted the order.<sup>374</sup> The petition website Change.org was also blocked the same month while it is

370 United Nations Special Rapporteur on the situation of human rights defenders, *They spoke truth to power and were murdered in cold blood: Analysis on the situation of environmental human rights defenders and concrete recommendations to better protect them*, (2016), p.19, available at: [https://www.protecting-defenders.org/sites/protecting-defenders.org/files/environmentaldefenders\\_0.pdf](https://www.protecting-defenders.org/sites/protecting-defenders.org/files/environmentaldefenders_0.pdf)

371 Prachatai, กลุ่ม นศ. แม่โจ้ ขอแรงช่วยชาวบ้านค้านเหมืองถ่านหินอมก๋อย จ.เชียงใหม่, 28 May 2019, available at: <https://prachatai.com/journal/2019/05/82688>; Northnews, “เสรีชนพนัส”ม.แม่โจ้ บุกอมก๋อย เตรียมช่วยชาวบ้านคัดค้านเหมืองถ่านหิน, 29 May 2019, available at: <http://www.northpublicnews.com/เสรีชนพนัส-บุก-อ-อมก/>; Prachatai, เรียก 4 นักศึกษาแม่โจ้รับทราบข้อกล่าวหาหมิ่นประมาทฯ ปมพาดพิงเหมืองถ่านหิน, 26 November 2019, available at: <https://prachatai.com/journal/2019/11/85312>

372 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020>

373 Human Rights Watch, *Thailand: Outspoken TV Channel Banned*, 21 October 2020, available at: <https://www.hrw.org/news/2020/10/21/thailand-outspoken-tv-channel-banned>

374 International Federation of Journalists, *Thailand: Court order to suspend online broadcaster revoked*, 23 October 2020, available at: <https://www.ifj.org/media-centre/news/detail/category/press-releases/article/thailand-court-order-to-suspend-online-broadcaster-revoked.html>; Prachatai, *Court lifts suspension orders against Voice TV*, Free Youth, 22 October 2020, available at: <https://prachatai.com/english/node/8863>

reported that access to the messaging app Telegram would soon be restricted with the aim to curb the democracy movement.<sup>375</sup>

The government uses legal, administrative or other means to force individuals, publishers and digital platforms to delete their content. There are frequent reports that the authorities have pressured online users to remove their posts.<sup>376</sup> Social media providers or intermediaries often opt to comply with removal requests to avoid criminal liability. From January to June 2020, Facebook restricted access in Thailand to 202 items in response to reports from the MDES alleging violations of lèse-majesté law and Section 14(3) of the Computer Crimes Act.<sup>377</sup> According to Google's transparency report, the government sent 37 requests from January to May 2020 to remove 1,362 items across various Google services, including YouTube.<sup>378</sup> Such requests are all related to criticism of the government. While Facebook announced legal response to such orders,<sup>379</sup> the MDES filed a legal complaint against Twitter and Facebook for failure to comply with takedown requests in September 2020, marking the first time in Thailand that the computer crime law is exercised to prosecute the service providers.<sup>380</sup> The blocking of websites and removal of online content curtail the right of IPs and IEHRDs to get access to unrestricted information, thereby undermining activities of IEHRDs and resulting in a lack of oversight on development projects and government plans affecting livelihoods of IPs.

#### 4.4 Violation of online privacy and anonymity

Concerns remain over privacy and surveillance under the existing legal and institutional framework of Thailand. Provisions of the CCA, the Cybersecurity Act, the PDPA and the National Intelligence Act give sweeping power to the government to access personal information without judicial review or other forms of oversight. Cybersecurity Act neither provides for notification to individuals, who could be affected by information gathering, nor places restrictions on the handling of the information to safeguard all personal information.<sup>381</sup> Data collected by the government on grounds of national security are exempted from privacy protections that are otherwise guaranteed under PDPA. In practice, it is reported that the government possesses various surveillance technologies allowing for information interception.<sup>382</sup> Recently, contact tracing apps were introduced by the government to stop the spread of COVID-19 whereas they reportedly contain excessive user permissions and

375 BBC, *Thailand blocks Change.org as petition against king gains traction*, 16 October 2020, available at: <https://www.bbc.com/news/world-asia-54566767> ; BBC, *Thailand protests: Authorities move to ban Telegram messaging app*, 19 October 2020, available at: <https://www.bbc.com/news/world-asia-54598956>

376 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020>

377 Facebook Transparency, Thailand, available at: <https://transparency.facebook.com/content-restrictions/country/TH>

378 Google, *Transparency Report Government requests to remove content, Thailand*, available at: <https://transparencyreport.google.com/government-removals/by-country/TH>

379 Prachatai, *Royalist Marketplace returns*, 25 August 2020, available at: <https://prachatai.com/english/node/8748> ; The Reuters, *Facebook says plans to challenge Thai government demand to block group critical of monarchy*, 25 August 2020, available at: <https://www.reuters.com/article/us-thailand-facebook-statement-idUSKBN25L0BR>

380 Bangkok Post, *Govt taking legal action against major social media providers*, 24 September 2020, available at: <https://www.bangkokpost.com/thailand/politics/1990975/govt-taking-legal-action-against-major-social-media-providers> ; The Reuters, *Thailand takes first legal action against Facebook, Twitter over content*, 23 August 2020, available at: <https://www.reuters.com/article/us-thailand-internet-idUKKCN26F0R7>

381 Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, September 2019, available at: <https://www.manushyafoundation.org/study-on-cybersecurity-act>

382 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020>

have terms and conditions lacking transparency.<sup>383</sup> The government has also restricted anonymity on the internet. Section 18(7) of the CCA enables officials to order individuals to decode any person's computer data without a court order.<sup>384</sup> Thus, the government regularly monitors social media and private communications and gathers information, not only raising significant privacy concerns but also leading to the information collected being misused to prosecute IEHRDs based on the content. Moreover, due to the delayed implementation of the PDPA and the lack of protection for cybersecurity risks posed on individuals, IEHRDs may also face risks of data breaches by the third party.

### Case of violation of online privacy of Malay Muslims

Starting in June 2019, Thailand's Internal Security Operations Command, a unit of the military, and telecom providers began contacting Malay Muslims across the southernmost provinces of the country requiring them to re-register their SIM cards with their faces scanned and checked alongside the data on their National ID cards. Those, who did not comply by April 2020, have reported targeted mobile network shutdowns in early May 2020 amid the pandemic.<sup>385</sup> Apart from the collection of biometric data, 8,200 surveillance cameras with Artificial Intelligence are reportedly to be applied in the southern border provinces this year to increase the efficacy of the authorities' "monitoring and risk notification system" in the name of "ensuring the local population's safety".<sup>386</sup>

## 4.5 Lack of effective remedies

In some cases of violations, State-based grievance mechanisms are available as IEHRDs can bring their case to courts or file complaints with the National Human Rights Commission of Thailand (NHRCT). Nevertheless, it has been observed that these channels are often ineffective.<sup>387</sup> In the context of digital rights, access to remedy is hindered by the law and the practice. The Cybersecurity Act does not provide for any remedy against the authorities for misuse, wrongful application or excessive action under this Act, resulting in impunity and lack of accountability. Specifically, access to remedy in the form of appeal in the case of critical level and crisis level cybersecurity threats, according to Section 69 of the Act, is prohibited.<sup>388</sup> Individuals and IEHRDs who could be subject to the incorrect interpretation and application of cybersecurity laws are less likely to have access to redress, thus in return fostering the climate of self-censorship.

- 
- 383 DPEX, *A Comparative Review of Contact Tracing Apps in ASEAN Countries*, 2 June 2020, available at: <https://www.dpexnetwork.org/articles/comparative-review-contact-tracing-apps-asean-countries/>; Bangkok Post, *Thai Covid-19 apps judged invasive*, 20 July 2020, available at: <https://www.bangkokpost.com/business/1954287/thai-covid-19-apps-judged-invasive>
- 384 Computer Crime Act B.E. 2560 (2017), available at: [http://web.krisdika.go.th/data//document/ext809/809777\\_0001.pdf](http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf)
- 385 Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: <https://freedomhouse.org/country/thailand/freedom-net/2020>; Civil Rights Defenders, *Thailand's Facial Recognition policy in the Deep South raises serious human rights concerns*, 18 June 2020, available at: <https://crd.org/2020/06/18/thailands-facial-recognition-policy-in-the-deep-south-raises-serious-human-rights-concerns/?fbclid=IwAR1Iz5MOg6bSJWNZDpgHFopHWOvujhVcjzibGTUEkSSpUAgZ8o7srKSE3c>
- 386 Asia Sentinel, *Thai Military Strategy in the Deep South: Surveillance State*, 1 June 2020, available at: <https://www.asiasentinel.com/p/thai-military-strategy-in-the-deep>; New Mandala, *The Patani Panopticon: biometrics in Thailand's deep south*, 27 May 2020, available at: <https://www.newmandala.org/the-patani-panopticon-biometrics-in-thailands-deep-south/>
- 387 Manushya Foundation and Thai Business & Human Rights Network, *The Protection of Human Rights Defenders*, 2019, available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_6d64d56d0f7c478298e000b18aed6f81.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_6d64d56d0f7c478298e000b18aed6f81.pdf)
- 388 Cybersecurity Act, B.E. 2562 (2019), available at: <https://cyrilla.org/en/entity/4nywjpircms?file=1588770279351q8g2xeaybw.pdf&page=1>

## 5. Recommendations

### 5.1 Recommendations to the government

**5.1.1** Ensure individual rights to online freedom and access to information are protected in line with international human rights law, including with respect to freedom of expression guaranteed under Article 19 of the UN Declaration on Human Rights and of the International Covenant on Civil and Political Rights (ICCPR);

**5.1.2** Revise existing laws to address all shortcomings including provisions that are broad, that violate human rights, that provide unchecked power, and that fail to acknowledge accountability and transparency in conformity with international human rights standards, as noted in Human Rights Committee Concluding observations on the second periodic report of Thailand (2017). The laws include the Emergency Decree, the Criminal Code, the CCA, the Cybersecurity Act, PDPA and the National Intelligence Act;

**5.1.3** Refrain from forcing tech companies as well as ISPs from taking part in government censorship and surveillance and permit them to comply with their responsibilities to respect human rights in line with the UNGPs;

**5.1.4** Provide a remedy against SLAPP cases, adopt standalone anti-SLAPP legislation or provisions that protect IEHRDs from intimidation and silencing of criticisms against businesses; end all ongoing legal proceedings against individuals facing charges, investigation or prosecution initiated by State authorities for engaging in legitimate activities protected by international human rights law or for addressing violations;

**5.1.5** End impunity of perpetrators responsible for serious human rights violations affecting the rights of persons and the work of IEHRDs - whether those are businesses or members of the government that contribute to violations by businesses;

**5.1.6** Set up accessible and appropriate, judicial and non-judicial grievance mechanisms and provide, among the remedies for abuses, fair treatment, just compensation and satisfaction, and the establishment of sufficient grounds to avoid recurrence of the abuses; regular review of the mechanisms must be carried out;

**5.1.7** Enhance awareness of Indigenous communities as well as the concerned government authorities and State bodies on the rights of Indigenous Peoples and challenges therefor in Thailand, such as through regular dialogues and interactions;

**5.1.8** Consult and cooperate in good faith with the IPs affected by development or other projects through their own representatives (such as IEHRDs) or institutions; require (FPIC) of IPs prior to any project affecting their lands, territories and resources in line with international human rights standards.

### 5.2 Recommendations to digital technology companies

**5.2.1** Ensure the companies' terms of service and policies are uniform and comply with international standards on freedom of expression and protection of data privacy, which are reviewed regularly to ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological and societal developments, in line with the obligation to respect human rights under UNGPs;

**5.2.2** Ensure that any requests, orders and commands to access information or remove

content must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary as well as proportionate means to achieve one or more aims;

**5.2.3** Publish regular information on their official websites regarding the legal basis of requests made by governments and other third parties and regarding the number or percentage of requests complied with, and about content or accounts restricted or removed under the company's own policies and community guidelines;

**5.2.4** Provide company-level remedies and grievance redressal mechanisms both physical and virtual, to victims affected by adverse impacts of cybersecurity responses that violate their rights; provide users with an opportunity to challenge decisions, particularly on the takedown of or access to their information when unlawful under national or international law; or if the restrictions are unfair and unduly restrictive.

## 5.3 Recommendations to project developers and investors

**5.3.1** Take all necessary and lawful measures to ensure that business practices do not cause, contribute or remain complicit in violations, with respect to the rights of IPs and IEHRDs;

**5.3.2** End all legal proceedings against individuals facing investigation, charges, or prosecution initiated by businesses for engaging in legitimate activities protected by international human rights law or for addressing violations;

**5.3.3** Conduct assessments and due diligence processes to determine the impact of business activities on IPs, with respect to individual and community rights; ensure full participation by and consultation of affected IPs and EHRDs;

**5.3.4** Disclose information related to planned and ongoing large-scale development projects in a timely and accessible manner to affected communities and IEHRDs;

**5.3.5** Establish and participate in effective non-State-based grievance mechanisms, including at operational levels.

## 5.4 Recommendations to IEHRDs

**5.4.1** Engage in the process of understanding digital threats to civic space; identify and document internal and external threats to the freedom of expression with respect to the legal framework;

**5.4.2** Use encrypted communication in daily works, and choose online platforms that allow users to send encryption-protected information to others and collect and store very little data about users to mitigate surveillance; ensure that the software versions are up to date and authentication inside and out is upgraded;

**5.4.3** Raise awareness of all judicial and non-judicial grievance mechanisms to seek redress in face of human rights violations;

**5.4.4** Increase engagement with business and the government in support of Indigenous rights and digital rights; provide recommendations on the implementation of cybersecurity laws and laws regarding IPs;

**5.4.5** Hold implementing authorities and officials liable for the misuse of their powers or information obtained while carrying out their duties under cybersecurity laws.





The background image shows three women from behind, walking on a dirt path. They are carrying large, rectangular, woven baskets on their backs. The woman in the center is wearing a colorful patterned shirt and a black skirt. The woman on the left is wearing a green long-sleeved shirt and a black skirt. The woman on the right is wearing an orange puffer jacket and a colorful striped skirt. They are walking away from the camera towards a misty, mountainous landscape.

# VIETNAM

Prepared by **Emilie Pradichit,**  
*Manushya Foundation*



# 1. Introduction

## 1.1 Profile of Indigenous Peoples in the country

Map of distribution of ethnic groups in Vietnam



Source: Country Policy and Information Note - Vietnam: Ethnic and religious groups", March 2018, available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/695864/Vietnam\\_-\\_Ethnic\\_and\\_Religious\\_groups\\_-\\_CPIN\\_v2.0\\_ex.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/695864/Vietnam_-_Ethnic_and_Religious_groups_-_CPIN_v2.0_ex.pdf).

Vietnam is a multi-ethnic country composed of 54 different ethnic groups. Ethnic Kinhs make up the overwhelming majority of the population, accounting for approximately 86.2%. The remaining 13.8% percent, or 13.4 million people, are divided between five main Indigenous Peoples (IPs) groups.

The IPs in Vietnam are generally found in communities located in mountainous areas or alongside the Mekong River, and livelihoods of most of them are based on agriculture. They are residing mainly in three geographical regions of the country (Please also see Figure 1):

▣ The North-west and North: the Tai or Thai (1.3 million people), the Tay (1.4 million people) and the Hmong (1 million people) living in the mountainous regions of Northern Vietnam.

▣ The Central Highlands: the Montagnards, also known as Degar (1 to 2 million people), are composed of no less than 30 ethnic minority groups and are most often referred to as "ethnic minorities in Tay Nguyen" by the State authorities.

▣ Delta region of the Mekong River: the Khmer Krong (1.3 million people)

## 1.2 Legal framework on the rights of Indigenous Peoples

Although present in very large numbers in Vietnam, none of these Indigenous groups enjoy formal recognition of their status under the national law. Despite voting in favor of the United Nations Declaration on the Rights of the Indigenous Peoples (UNDRIP), Vietnam does not recognize Indigenous Peoples as such, and neither has it ratified the International Labour Organization (ILO) Convention 169. In its third periodic report submitted to the Human Rights Committee (HRC) in 2017, Vietnam declared that no Indigenous Peoples or Indigenous issues

were found in the country. The government uses the term “ethnic minorities” to refer to them. These statements clearly illustrate the government’s failure to recognize, and respect their identities, history and rights.

All IPs are “full citizens of the Vietnamese state and enjoy constitutionally guaranteed rights to their languages and cultural traditions”. Hence, the legal rights of Indigenous Peoples in Vietnam compare favourably with those of other South-East Asian countries. Under Vietnamese law, all ethnic minorities enjoy citizenship. They are also guaranteed equal rights and protection under the Constitution (Article 5). Nevertheless, the reality is much different. The lack of formal recognition of their Indigenous status leaves rights under-protected and often abused. There is no specific law on Indigenous Peoples, but the Committee on Ethnic Minorities Affairs is a ministerial-level entity in charge of advising the National Assembly and the Ethnic Council on ethnic minority issues and to manage, control and oversee the implementation of the government’s ethnic minority policies and development programs in ethnic minority areas.

Besides, in spite of the many development policies implemented by the Vietnamese authorities over the years, Indigenous Peoples are significantly poorer than the majority population. In 2015, for instance, the poverty rate registered for ethnic minorities was 23.1%, while the national poverty rate was 7%. With poverty comes more issues, such as malnutrition, illiteracy and health issues – problems that particularly affect women.

Further, Amnesty International has highlighted that Indigenous Peoples are often being harassed by State authorities for speaking about their rights or merely for expressing a critical opinion towards the government’s actions or the Party. Some Indigenous communities are also persecuted due to their history, ethnicity or their religious beliefs. For instance, the Montagnards have long been persecuted for their connections with the French during the war and for their religious beliefs. Therefore, the vast majority of these Indigenous communities do not dare to speak out against the authorities anymore. Finally, Indigenous Peoples are also victims of stigma and discrimination, notably being presented as “backwards” and “superstitious” peoples.

### 1.3 The situation of Indigenous Environmental Human Rights Defenders (IEHRDs)

As the legal and institutional framework has generally failed the Indigenous communities, IPs and activists in Vietnam continue to fight for land and Indigenous rights. However, they experience barriers in accessing information, and the right to freedom of expression is often violated. With the civic space restricted by the State authorities in Vietnam, HRDs and activists have increasingly been using digital platforms and social media for advocacy, and to communicate, coordinate and store their information. According to Amnesty International, as of 2019, 64 million Vietnamese are regular internet users. Other sources estimate that Vietnam accounts for more than 60 million Facebook users - a platform widely used by HRDs, as it is one of the main sources of independent news. COVID-19 pandemic has considerably accelerated this process of migration of activism works from offline to online space and made connectivity a real necessity. HRDs now communicate, advocate, attend and participate in all kinds of online events, from workshops and training to international conferences. They also keep data, sometimes extremely sensitive, online. In this regard, as reported by the Amnesty International, Trinh Ba Phuong, a land rights activist and HRD, has declared that “the internet, especially social media, has transformed Vietnamese society

significantly. It gives people the ability to make their voices heard and [has] put an end to the government's domination over news and information. Now, everyone can be a journalist and publish whatever they want with just a Facebook account".

In response to this, the Vietnamese government has gradually enacted a set of repressive cyber-laws and policies that criminalize the sharing of information deemed critical of the government. They use "national security" - a term loosely defined under the National Security Law No.23/2004/QH11 - as a justification for their actions. For instance, during the pandemic, the Department of Information and Communications investigated more than 650 people and fined more than 160 people for sharing alleged "misinformation" in relation to COVID-19, which they were also forced to delete. In addition, 47 bloggers, activists and journalists were arrested for their online activities and placed in pre-trial detention. The year 2020 has also seen a rise in the number of prisoners of conscience – defined as individuals jailed because of their identity or beliefs, as per the Amnesty International. The number reached 170 – the highest figure ever recorded by the organization. Among them, at least 69 were imprisoned due to online activism and 30 were women. The government also implemented a few internet disruptions, notably a shutdown between February and April 2020 – thereby restricting the flow of information even further. Vietnamese authorities have also forcefully secured the cooperation of internet providers and tech companies, making online surveillance and information take-downs widespread.

This has led to the silencing and systemic harassment of HRDs, including IEHRDs. They are frequent victims of threats, intimidation, arbitrary arrests, prosecution and legal punishments. This reliance on technology has also resulted in cyberattacks and online monitoring and surveillance. For instance, a 2018 research by eQualitie, a group that aims to create accessible technology to promote and defend human rights on the Internet, revealed that the website Tiếng Dân, an independent media, suffered several distributed denial-of-service (DDoS) attacks from April to June 2018. Similarly, the Facebook page of the Liberal Publishing House was repeatedly attacked in 2019, leading to its closure. Due to these increasingly tough restrictions on online freedom that expose online activities to growing threats of shaping narratives, censorship and surveillance, the Reporters Without Borders ranked Vietnam 175 out of 180 countries on its 2020 World Press Freedom Index. Similarly, the Freedom House labelled Vietnam as "not free" when it comes to online freedom and CIVICUS Monitor rated Vietnam's civic space as "closed". In addition, a report published by the Reporters without Borders in December 2020 revealed that Vietnam is among the countries with the largest number of journalists and Facebook behind the bar, along with China, Egypt, Saudi Arabia and Syria. The organization estimates that 7 journalists and 21 Facebook users are imprisoned in the country. Likewise, the Committee to Protect Journalists argues that 15 journalists are jailed in Vietnam – a figure which the government rejects. During its 2<sup>nd</sup> Universal Periodic Review cycle, Vietnam received six recommendations related to the protection of HRDs, freedom of expression and access to information. However, to this day, it has failed to implement the overwhelming majority of the recommendations, showing a clear disregard for the right to information and expression.

## 2. Methodology

The methodologies used for this report include desk research, interviews and consultations with IEHRDs at local and national levels. Manushya Foundation gathered Primary sources, including voices, concerns, cases and experiences of the IEHRDs. The RightsCon 2020 panel session on “Will democracy survive ‘national security’ in the digital spaces of Southeast Asia”, hosted by Manushya Foundation and PEN international on 31 July 2020, also informed the knowledge of this document. RightsCon is a global summit on human rights in the digital age, gathering various stakeholders, such as leading voices of experts, academics, business leaders and advocates working on the ground. This report is also based on desk research including a systematic literature review of relevant laws and government regulations; reports and observations/recommendations of UN human rights bodies and NGOs; online news articles; expert papers and other publications. It aims to present an analysis of the legal framework on cybersecurity laws and potential impacts on IEHRDs.



Women are threshing rice in Xã Lao Chải, H. Sa Pa, Vietnam



### 3. Legal and Policy Framework in Relation to the Rights of IEHRDs in Digital Age

#### 3.1 Constitutional provisions and laws stipulating the rights of IEHRDs

**HUMAN DEVELOPMENT INDEX (HDI):** 0.704 (2019)  
**NUMBER OF INTERNET USERS IN VIETNAM:** 68.72 million (as of January 2021)  
**LEVEL OF FREEDOM:** 19/100 (with 0 being least free and 100 being most free, Freedom in the World 2021 – Freedom House)  
**LEVEL OF PRESS FREEDOM:** Ranked 175<sup>th</sup> out of 180 countries (with 1<sup>st</sup> being highest level of press freedom, World Press Freedom Index 2021 - Reporters Without Borders)  
**LEVEL OF FREEDOM ON THE NET:** 22/100 (with 0 being least free and 100 being most free, Freedom on the Net 2020 – Freedom House)  
**GLOBAL CYBERSECURITY COMMITMENT:** Ranked 25<sup>th</sup> out of 182 countries with a score of 94.59/100 (with 1<sup>st</sup> being highest and 182<sup>nd</sup> being the lowest commitment – ITU Global Cyber Security Index)

The State of the Socialist Republic of Vietnam recognizes, respects, protects and guarantees human rights and citizens' rights as per Article 3 of the 2013 Constitution. Article 5 of the Constitution affirms equality and unity among all the ethnicities of Vietnam and prohibits discrimination against them, and that the State shall implement a policy of comprehensive development and create conditions for minority ethnicities to fully utilize their abilities to develop together with the nation.

Article 14 of the Constitution states that "political, civic,

economic, cultural and social human rights and citizen's rights are recognized, respected, protected and guaranteed in concordance with the Constitution and the law" and that they "shall only be restricted in imperative circumstances for the reasons of national defense, national security, social order and security, social morality, and the health of the community". Article 16 of the Constitution ensures that all citizens are equal before the law while Article 17 forbids expelling a Vietnamese citizen. Article 20 of the Constitution states that all individuals shall be protected against torture, harassment and coercion, as well as against "any form of violation of his or her life and health, and offence of honor and dignity". It also guarantees that no one shall suffer from arrest in the absence of a court's decision. Article 30 and 31 of the Constitution respectively allow citizens to lodge complaints for violations of their rights and provide for reparation, a procedure that is dealt with in Chapter XXXIII of the Criminal Procedure Code; and to the right of fair trial and to be defended by a lawyer. Freedom of religion is guaranteed under Article 24 of the Constitution, and under Article 164 of the Criminal Code, although many Indigenous Peoples see this right being largely violated under Article 5 of the 2018 Law on Belief and Religion, which allows the government to reject religious activities that "infringe upon national security" or represent a violation of social morality.

Several constitutional provisions and laws also affirm the right to privacy. For instance, Article 21 of the Constitution protects personal privacy and secrecy, including that of correspondence, telephone, telegrams and other forms of exchange of personal information and is therefore applicable to the digital sphere. It also forbids the confiscation and control of other's personal information and does not provide any exceptions for that. Similarly, Article 38 of the Criminal Code guarantees the right to privacy by stating that the collection, storage, use and disclosure of personal information requires the individual's consent and that private exchanges are safe and confidential. Article 159 of the Code condemns the infringement upon "secret information, mail, telephone, telegraph privacy, or other means of private information exchange". In addition, the Law on Information Technology No.67/2006/QH11, the Law on Telecommunications No.41/2009/QH12, the Press Law No.103/2016/QH13 and the Law on Access to Information and the Law on Cyberinformation Security No.86/2015/QH13 mention and specify the right to privacy and the protection of personal information, and prohibit any acts of infringement of the right to privacy in post and telecommunications activities, the safety of information, and application and development of information technology.

Articles 23 to 25 of the Constitution and 167 of the Criminal Code provide for the rights to freedom of movement and residence, belief and religion, opinion and speech, press, as well as to access to information, to assemble, form associations and hold demonstrations. Besides, under Articles 10 and 11 of the Press Law, citizens have the right to freely express opinions about the situation of the country and the world, and to access information in the press. Article 13 of the Press law further states that it is the State's responsibility to "create favourable conditions for citizens to exercise their rights to freedom of the press and freedom of speech in the press". Under Article 4 of the Law on Access to Information, all citizens are equal and free from discrimination in accessing information. The law also guarantees that restrictions placed upon the right to access information can only be valid when provided by the law, such as on grounds of national defense and security, social order and safety, social ethics or community well-being. The Criminal Code includes provisions for punishing cyberattacks, such as Article 286 that sets out a fine of a maximum 200,000,000 VND and 36 months of imprisonment for "spreading software programs harmful for computer networks, telecommunications networks, or electronic devices", or Article 287 and 289 that criminalizes the "obstruction", "disturbance" and "illegal infiltration" of these networks and devices.

Despite these explicit provisions, challenges remain in peacefully exercising the rights to freedom of expression and assembly as well as to privacy and access to information, along with ensuring the participation of IPs and IEHRDs affected by development projects and business conduct. Many restrictive laws fall short of international standards for the rights of IPs and IEHRDs.

## 3.2 Legal framework restricting offline activities of HRDs

### 3.2.1 Criminal Code

Amended in 2015, the Criminal Code is widely used to clamp down on freedom of expression, especially under its Articles 117, 118 and 331. The Code is implemented by police authorities, the People's Procuracies (public prosecutors) and People's Courts as well as the Ministry of Justice. According to Article 117, making, storing or sharing of distorted or fabricated information about the government can be punished with between 5 to 12 years in

prison. Article 118 forbids the incitation, persuasion or gathering of people for the purpose of opposing the government and disrupting national security; and punishes those acts with imprisonment of between 2 and 15 years. Both articles also criminalize the “preparation” of this criminal offence with jail sentences. Further, Article 331 condemns the “abuse of democratic freedoms”, such as freedom of speech, of the press, of religion, of association, and other freedoms to violate State interests, which is punishable with up to 7 years of prison.

The Articles 118 and 331 are in violation of the international human rights law, notably Article 19 of the International Covenant on Civil and Political Rights, which provides for restriction on freedom of speech on some grounds, including that of “national security” or “public order”, but the Human Rights Committee, in its General Comment No. 34, has noted that those grounds cannot be excessively used as a legitimate reason. Article 331 has very often been used to infringe upon the right to freedom of expression online. Since the introduction of the Criminal Code in 2015, 21 people have been charged under the Article and 11 persons were sentenced with jail terms for online Facebook posts.

While the above Articles of the Criminal Code are the most widely used to clamp down on online dissent, some other provisions are also frequently used to silence HRDs and IEHRDs. Those include Article 109 that criminalizes “activities against the people’s government”, which is punishable by up to life imprisonment or death penalty, and Article 318 on the disturbance of “public order”. Further, the language used throughout the Criminal Code is extremely broad and vague, citing offences that are undefined, such as “spying” (Article 80) or “circulating propaganda against the Socialist Republic of Vietnam” (Article 88).

### **3.2.3 Press related laws: 2005 Decree No.38, 2011 Decree No.2 and 2016 Press Law**

The 2016 Press Law, implemented by the Ministry of Information and Communication, considers the press to constitute the “voice of the Party, of State and social organizations” (Article 4), hinting at State’s control over the media and critical voices. The 2011 Decree No.2 gives the State the authority to punish journalists and bloggers for various activities and behaviors, including that of using a pseudonym to publish. Similarly, the 2005 Decree No.38 bans gatherings outside state agencies and public buildings, as well as all protests deemed to interfere with the political activities or the State or the Party. In addition, Public Security Circular 09/2005/TT-BCA that serves as implementing guidelines to the Decree forbids gatherings of more than five people without prior state approval. Both these regulations were used to repress the 2018 massive demonstrations against the Special Economic Zones and Cybersecurity Law drafts.

## **3.3 Cybersecurity Laws and policies restricting online activities of IEHRDs**

### **3.3.1 Decree No.72/2013/ND-CP on the Management, Provision and Use of Internet Services and Online Information**

Enacted in 2013, the Decree specifically prohibits online information that is deemed to “oppose the State”, “undermine the national security, social order and safety”, “sabotage the great national unity bloc”, as well as information considered to be state secrets, slanderous or defamatory (Article 5). It mandates internet-based service providers, including social

media, to cooperate with the State authorities, notably the Ministries of Public Security and of Information and Communications, to delete online content. Offshore internet-based service providers, such as Facebook or Google, are also obliged to locate at least one server in Vietnam (Article 24). In addition, social media companies are required to “register, store and manage personal information of the persons that establish private websites and other information providers on social networks” (Article 25(9)). This provision, which is similar to one of the Law on Cybersecurity provisions, considerably threatens online privacy and heightens the risks of State-led harassment of HRDs and activists.

Further, this decree could soon become even more restrictive. An amendment to the decree was drafted in April 2020 by the Ministry of Information and Communications. If voted, it could impose further restrictions upon companies. Article 23.d of the draft amendment is especially problematic as it notably proposes to establish a mechanism for removing illegal content within three hours upon the Ministry of Information and Communications’ request, or to block any content presented as journalistic products. The draft also threatens to expose personal data and information of social media users, which would considerably increase the risks of harassment and State persecution. This draft amendment has therefore been strongly opposed by both the private and public sectors.

### 3.3.2 2018 Law on Cybersecurity (LOCS)

Enacted in 2018, the LOCS was directly developed from Decree No. 72 and came into effect on 1 January 2019. It is being implemented by the Ministry of Information and Communication and the Ministry of Public Security, except for matters falling under the Ministry of Defence’s responsibility and the Cipher Department. It is the first comprehensive law on cybersecurity enacted in Vietnam, as previous regulations were divided into many different legislations. The law raised many concerns not only among civil society actors and the international community but also in the private sector for giving sweeping power to the government. Under Articles 8 and 16, developing, posting and sharing of distorted and fabricated information for the purpose of propaganda or defamation is strictly forbidden. The same applies to information that represents a security risk for the country, or that may disrupt public order. Article 17.1.d is equally problematic as it forbids divulging State secret - a concept which lacks precise definition under Vietnamese law.

Additionally, Articles 16 and 26 impose restrictions on big tech companies and other internet-based service providers. Under these provisions, companies must comply with requests of the Cybersecurity Taskforce, acting as part of the Ministry of Public Security, regarding content takedowns or sharing of users’ data. For instance, although Article 26 mandates companies to authenticate user information and keep them confidential, it also requires companies to provide such information to the Cybersecurity Taskforce upon investigation. According to Amnesty International, this allows the Ministry of Public Security to gather information without any stated requirement for a warrant or judicial oversight. Content deemed critical of the government or harmful to national security must be removed within 24 hours - once again with no checks and balances from the judiciary. These provisions also state that companies are responsible for the prevention, monitoring and removal of content deemed in violation of the law. That, as per Amnesty International, creates “an incentive for excessive censorship, seemingly without any procedural safeguards such as independent judicial oversight”. Finally, they mandate companies to refrain from providing services to certain individuals, upon the Cybersecurity Taskforce requests, if they have shared content

deemed in violation of the law; and to locate at least one server in Vietnam – a step meant to facilitate government's access to users' data.

The law makes it unclear whether people charged under it have access to any legal recourse for appeal. Throughout the LOCS, an absence of independent oversight, redress and accountability mechanisms is evident. Orders by a court or any other independent body are not required for State authorities to penalize companies which fail to comply with censorship obligations, cybersecurity audits, reporting requirements, obligations to furnish user data or data localization requests. There is also no provision for appeal or judicial review of orders made by the MPS or MIC under the law.

### **3.3.3 2016 Circular No.38**

The 2016 Circular No.38 of the Ministry of Information and Communications sets out a process by which internet-based service providers located outside of Vietnam must cooperate with State authorities to combat online content deemed “bad” and “toxic”.

### **3.3.4 2020 Decree No.15**

The 2020 Decree No. 15, which was enacted in February 2020, sets out the penalties for violations of regulations imposed on “postal services, telecommunications, radio frequencies, information technology and electronic transactions”. This decree replaced former Decree No.174 and lists a number of administrative offences for which both users and internet service providers can be punished. For instance, Article 100, which specifically applies to “social networking sites”, provides for the suspension of a company's license, if the latter fails to provide user data accused of “being involved in terror acts, crimes or other violations against law at the request of competent authorities” or for failing to remove information deemed in violation of Vietnamese law. It also imposes a penalty ranging from 50 to 70 million VND (between 2,130 and 3,000 USD) for companies storing or sharing fabricated or untruthful information that is harmful to the national interests or defamatory. These penalties have raised concerns as they incentivize companies to proactively apply self-censorship and curtail freedom of expression in the country. Article 101, on the other hand, targets internet users. Those accused of posting or sharing fake news, fabricated, distorted or slanderous information, or promoting superstition or practices that are not in line with Vietnamese customs, can be fined anywhere between VND 10 million (approx. US\$ 430) and VND 20 million (approx. US\$ 860). The Decree has been especially used during COVID-19 to fine individuals for misinformation and fake news spread on the pandemic and its handling by the government.

### **3.3.5 Law on Access to Information**

Enacted in 2016, this law is also being used to restrict online freedom, and especially the right to information and to freedom of expression. This law denies citizens' access to information deemed to be harmful to State interests, national defense and security. At the same time, it grants the State authority to punish activists and journalists sharing any information considered as a critique or being defamatory to the State.

## 4. Challenges on the ground: Impacts of Cybersecurity Laws on IEHRDs and Significant Cases

### 4.1 Threats and harassment for online activity

IPs and IEHRDs, who express dissenting views online in Vietnam, have faced harassment, intimidation, arrest and prosecution by the authorities, notably under the Criminal Code. When IPs are being targeted, many arrests are also carried out under charges such as “dissemination of propaganda against the state” or “activities to overthrow the government” and result in harsh penalties – mostly between 10 and 20 years of imprisonment. Thus, the risk of severe criminal charges and targeted harassment or violence have discouraged IEHRDs from exercising their right to freedom of expression in practice. Additionally, the government has been reported to carry out massive surveillance operations and online espionage. As per the Amnesty International, Nguyen Lan Thang, an HRD from Ha Noi, has reported the existence of “public opinion shapers”, such as Force 47, that act under the authority of the Department of Propaganda since 2013, and exercise massive surveillance, monitoring and trolling of any individual deemed to be critical of the government online. He reports having been sent threats of all kinds, including death threats. State authorities have also supported online espionage and surveillance activities. FireEye, a foreign cybersecurity firm has also revealed that OceanLotus, a group of cyberspies, has targeted online HRDs and journalists.

#### Case of “Working sessions”

In its “Let us Breathe!” report, Amnesty International has unveiled that, in March 2017, the police summoned 700 people under Decree No.15 for interrogation sessions over their social media usage and their alleged circulation of “fake news” on COVID-19. These people were required to formally promise to refrain from committing such actions under the threat of legal actions, fines and jail sentences.

#### Case of activists charged for speaking out about the Formosa disaster

In November 2019, the EHRD Nguyen Ngoc Anh received a six-year jail term for reporting on the Formosa toxic spill. He was charged under the LOCS for allegedly “making, storing, releasing and circulating information and documents against the state”. In April 2020, HRD Dinh Thi Thy Thuy was arrested and charged under Article 117 of the Criminal Code for using her Facebook account to share her opinions on the Formosa environmental disaster in 2016, among other sensitive topics, and about the cybersecurity law in 2018. She also discussed environmental issues, notably with regards to her hometown, and she criticized some aspects of the government’s handling of the pandemic in 2020. As of the day of writing, she remains in pre-trial detention and faces up to 12 years of imprisonment.

#### Multiplication of cases in December 2020

In December 2020, in the span of two weeks (December 9-20), several HRDs were charged and convicted under various provisions of the Criminal Code. On December 15, the 68-year-old famous HRD Tran Duc Thach was charged with subversion under Article 109 of the Criminal Code for belonging to an unregistered group campaigning for democracy,



the Brotherhood for Democracy, which he co-founded. According to Nghe An Province authorities, he was posting and sharing articles on Facebook that were distorting the government's actions and policies while he was merely reporting corruption and human rights violations. The People's Court of Vietnam sentenced him to 12 years of prison and three years of probation.

The following day, the authorities of Can Tho City (Mekong Delta region) charged Truong Chau Huu Danh, a well-known 38-year-old Facebook user, under Article 331 of the Criminal Code for "abusing democratic freedom". He was targeted because of his intense activism online. Indeed, he is the creator of the Bao Sach (Clean Newspaper) Facebook page, which notably reports on human rights abuses, such as the unfair death sentencing of Ho Duy Hai. On December 21, Huynh Anh Koa and Nguyen Dang Thuong, two Facebook users were also tried under Article 331 of the Criminal Code for "abusing democratic freedom". They were arrested in June 2020 for their role in administering an open Facebook group (Bàn luận Kinh tế-Chính trị) centered on discussing socio-economic issues in the country. The Facebook group was closed after their arrests. If convicted, they face up to 7 years in prison.

## 4.2 Limited access to information caused by blocking and removal of content online

The Vietnamese authorities excessively control critical content online by blocking webpages and virtual private networks (VPNs) and requiring major companies such as Google, Twitter, and Facebook to remove content from their platforms. Although social media companies and internet-based service providers, such as Facebook and Google resisted State requests at first, they have been increasingly coerced into cooperating with the authorities. State authorities pressured them, notably by restricting the internet or shutting it down temporarily. In late 2017, the Minister of Information and Communication declared that Google had "removed 4500 videos containing bad or toxic content from YouTube" out of 5000 deletions requested by Vietnam while Facebook complied with 159 requests of the government regarding the removal "anti-government accounts". After having experienced a 7-week disruption of its services between April and June 2020, Facebook also recorded a 983% increase in compliance with Vietnam's requests in the first half of 2020. Facebook's censorship continues despite the company's public commitment to implement the United Nations Guiding Principles (UNGPs), which calls for businesses' responsibility to respect human rights. In the current COVID-19 context, this trend is particularly worrying as people are extremely dependent on the internet for information.

The following two cases are particularly emblematic of the poor digital rights situation in Vietnam for IEHRDs as well as the collusion between online crackdown on dissent and the physical risks they entail for activists. It also highlights the role of big tech companies in censorship in the country.

### Case against Nguyen Van Trang

Nguyen Van Trang is a HRD and member of the Brotherhood for Democracy, who is very active on Facebook. When interviewed by the Amnesty International, he reported that he experienced content restrictions starting in April 2020. Firstly, Facebook notified him that one of his posts was inaccessible to other users in Vietnam due to "local legal restrictions". He then noticed that all of his posts mentioning Nguyen Phu Trong and Tran Quoc Vuong - two figures of the Party - were systematically censored. According to him, Facebook's

compliance and cooperation with the State authorities' requests has forced him and many other HRDs and IEHRDs into self-censorship.

#### **Dong Tam case**

In early January 2020, a land dispute that had been going on for a while was repressed when the police stormed the community village of Dong Tam nearby Hanoi. Confrontations resulted in the death of three police officers and the 84-year-old village leader. The incident went viral on social media with many people sharing pictures, videos and critical posts. Before and after the incident the government suspended both the internet and telephone networks to restrict the sharing of information, and deployed Force 47, a cyber-army run by the Ministry of Public Security, to block and counter social media deemed critical of the way authorities handled the situation. Facebook was also seemingly involved in censoring Facebook accounts, for example, in the case of Bui Van Thuan, who received a company's notification that his posts were violating the Community Standards. Although he tried to appeal the company's decision, Facebook ignored his attempts until the company gave in to civil society pressure. Facebook also restricted the profiles of people attempting to seek more information about the incident. Several land rights activists were arrested for their online activism, including Can Thi Theu, Trinh Ba Phuong, Trinh Ba Tu and Nguyen Thi Tam and charged under Article 117 of the Criminal Code.

### **4.3 Lack of effective remedies**

Under the existing laws, IPs, HRDs and IEHRDs in Vietnam whose rights have been violated have no real access to an independent judicial or redress mechanism. In addition, some of them, most notably IPs, are often reluctant to seek remedies with State agencies and bodies due to many barriers, including language and fear of reprisals. Most of the complaints are not taken seriously by the authorities.



Living in the beautiful valley in Lao Cai, Vietnam

## 5. Recommendations

### 5.1 Recommendations to the government

**5.1.1** In line with the 2019 recommendations of the UN Human Rights Committee on the third periodic report of Vietnam, the government must repeal or substantially amend the Criminal Code provisions that criminalize or unduly restrict freedom of expression – both online and offline. Those provisions include Articles 109, 116, 117 and 331 of the 2015 Criminal Code. In reviewing those articles, special attention must be paid to ensure that language used is clear and specific, particularly in relation to concepts of “national security” or “public order” that must be well-defined and in line with Article 19 of the International Covenant on Civil and Political Rights.

**5.1.2** Vietnam must review the content of all its internet-related laws, and in particular decrees No.15, No.72 and No.174 as well as Article 8, 16, 17 and 26 of the LOCS in line with international human rights laws and standards, including the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights and the Human Rights Committee’s General Comment No.34 (2011). Specific attention must be paid to provisions that are overly broad or constitute gross human rights violations, and the review should also focus on providing checks and balance and accountability mechanisms to hold relevant authorities responsible in case of violations of human rights. Vague concepts such as “national security” or “public order” should be clearly defined in line with standards on online freedom guaranteed by the UDHR and ICCPR. In order to do so, the Vietnamese authorities must coordinate and cooperate with all affected stakeholders, including from the civil society and private sectors, in order to embrace a more human-based rights approach to cybersecurity.

**5.1.3** The Vietnamese government must refrain from pressuring private companies through legal or extra-legal means to unnecessarily or disproportionately place restrictions upon internet users’ rights. This requires the State to stop restricting the internet or deliberately slowing the internet traffic in order to coerce private companies to cooperate with their content removal requests. The authorities must also repeal or amend all articles imposing undue requirements on private companies, such as Articles 16 and 26 of the LOCS, that compel internet or tech companies to disclose personal data without adequate safeguards to prevent abuses.

**5.1.4** In line with the 2019 recommendations of the Human Rights Committee and the UN Declaration on Human Rights Defenders, the government must ensure that human rights defenders and other civil society actors are protected both offline and online against threats, intimidation and physical attacks. Vietnam must therefore recognize, support and protect the work and legitimacy of HRDs, including of IEHRDs, to ensure that they will not face risks or reprisals while defending the rights of their communities and the environment. In that regard, Vietnam must adopt the provisions in the UN Declaration on Human Rights Defenders as binding national legislation and consequently develop appropriate protection mechanisms as well as grievance mechanisms. In that regard, Vietnam must also fully cooperate with the relevant UN Special Procedures, including the UN Special Rapporteur on the situation of human rights defenders, by accepting their requests to visit the country. This also requires Vietnam to end the practice of incommunicado detention, solitary confinement, torture and other ill-treatment suffered by HRDs in prison in line with the UN Standard Minimum Rules for the Treatment of Prisoners (the Mandela Rules) or with the country’s own commitment under Article 20 of the Constitution and Article 10 of the Criminal Procedure Code.

**5.1.5** The State authorities must set up appropriate judicial and non-judicial redress mechanisms for cases of human rights violations and ensure their accessibility to all peoples. Specific attention must also be paid to ensure that barriers limiting access to effective remedies for Indigenous Peoples are removed, such as limitations of language. A regular review of these mechanisms must be carried out. Vietnam must also ensure that it conduct impartial investigations into all cases of rights violations and that it effectively prosecutes perpetrators.

**5.1.6** The Vietnamese government must refrain from using the state of emergency as an excuse to illegitimately restrict access to information and freedom of expression, especially in times of a pandemic. This requires the State to notably stop restricting the internet or deliberately slowing the internet traffic and to stop censoring information spread online about the COVID-19 or its handling by the authorities. This is also in line with the right to health under Article 12 of the International Covenant on Economic, Social and Cultural Rights, to which Vietnam is a state party, that guarantees access to health-related information and that therefore implies that State must not censor any related content.

**5.1.7** The State authorities should provide training to competent officials and authorities on the implementation of the LOCS and all other related laws, as well as on cybersecurity and digital rights, notably using global good practices.

**5.1.8** Vietnam must drop all charges against individuals, who are being prosecuted under repressive legal provisions, including of the Criminal Code and of the LOCS, for the exercise of their rights to freedom of expression online and offline and of peaceful assembly. It should also immediately and unconditionally release all prisoners of conscience, who have been imprisoned on those legal grounds.

**5.1.9** The Vietnamese government must adopt the standards prescribed in the UN Declaration on the Rights of Indigenous Peoples as binding national legislation in order to formally recognize the identity of Indigenous Peoples as well as their rights and ensure their dignity and wellbeing. At the same time, Vietnam must also ratify the Indigenous and Tribal Peoples Convention of the ILO (Convention No.169). That includes the need to ensure that Free, Prior and Informed Consent (FPIC) of the Indigenous Peoples is obtained for decision-making on matters affecting them and thus safeguard their way of life and protect them from forceful evictions or any other threats to their livelihoods.

## **5.2 Recommendations to digital technology companies**

**5.2.1** All private companies, including tech companies and inter-based service providers must ensure that all content moderation requests they receive from State authorities comply with international human rights laws and standards governing freedom of expression, and that they are made in writing pursuant to a valid legal order following due process and the principles of legality, necessity and proportionality. They must also refuse to hand over user data that could be used to persecute or endanger HRDs or any users exercising their human rights.

**5.2.2** They must ensure a fair and transparent moderation of the online content published on their platforms. This requires the following: the prioritization of users' right to freedom of expression and access to information, the clarification of applicable restrictions to such rights in the form of uniform terms of services and policies; and the rationale behind it, the notification of third parties and individuals affected by content removal or blocked account. Companies must also consider, when possible, alternative options to deletion and removal such as fact-checking and labelling. They must equally provide users with a platform or mechanism to challenge decisions affecting their access to information or freedom of speech and make reports on online takedowns and other restrictions available to the public.

**5.2.3** Tech companies and internet-based service providers must adhere to the UN Guiding Principles on Business and Human Rights and conduct impact assessments of and due diligence on their activities. This will help ensure that they are committed to upholding the rights of their users and that they take all necessary measures when identifying adverse effect.

## 5.3 Recommendations to IEHRDs

**5.3.1** In cooperation with State authorities and the private sector, IEHRDs and HRDs should set up an independent multi-stakeholder body to review and monitor the implementation of the LOCS and to provide recommendations, including with a view to adopting approaches that cause the least harm to individuals' rights, and to ensure the proper use of the principles of necessity and proportionality, and to promote a human rights-based approach to cybersecurity.

**5.3.2** IEHRDs should conduct research on and raise awareness about censorship and content manipulation, notably by investigating and exposing State propaganda campaigns. This will help Vietnamese people to take actions for enhancing online freedom and protecting themselves against the risks incurred.

**5.3.3** IEHRDs should use strategic litigation to push back against shutdowns and censorship. Some successful examples can be found in Asia, notably in Indonesia and India. They should carefully assess whether to directly bring the case to the courts or to support other people's case as such processes can be lengthy, cumbersome and costly. An alternative can be to provide friend-of-the-court filings that explain how certain forms or uses of digital technology undermine human rights.

**5.3.4** HRDs and IEHRDs, including Indigenous Peoples, must participate, whenever possible, in training and workshops organized by civil society actors in order to strengthen their resilience and ability to prevent or cope with cyber threats. Such examples include the regional exchange and training on digital security for Indigenous HRDs that AIPP organized between 30<sup>th</sup> September and 2<sup>nd</sup> October; Manushya's "Increasing Digital Literacy in Thailand" project, which focused on knowledge on digital risks and threats, digital tools, and training ability; or Frontline Defenders' digital workshop that helps civil society actors and HRDs to "more effectively assess needs and identify digital risks, help design tailored security policy and cooperate in implementing it and integrating the practices into daily work and life". Frontline Defenders has also created a Security-in-a-Box tool – a compilation of guides and free and open-source tools that are meant to help HRDs securing their digital/online tools such as phones or computers and enhance their digital security. The tool is notably also available in Vietnamese.

# References

- Adam Bemma, *Vietnam's battalions of 'cyber-armies' silencing online dissent*, Al Jazeera, (17 January 2020), available at: <https://www.aljazeera.com/news/2020/1/17/vietnams-battalions-of-cyber-armies-silencing-online-dissent>.
- Amnesty International, *Big Tech's Censorship Shame in Viet Nam*, (December 2020), available at: <https://www.amnesty.org/en/latest/research/2020/12/vietnam-let-us-breathe/>.
- Amnesty International, *Surveillance giants: How the business model of Google and Facebook threatens human rights*, (2019), available at: [https://www.amnesty.ch/de/themen/ueberwachung/dok/2019/ueberwachung-durch-facebook-und-google/191121\\_rapport\\_fb\\_google\\_surveillance-docx.pdf](https://www.amnesty.ch/de/themen/ueberwachung/dok/2019/ueberwachung-durch-facebook-und-google/191121_rapport_fb_google_surveillance-docx.pdf).
- Amnesty International, *Viet Nam 2019*, (2019), available at: <https://www.amnesty.org/en/countries/asia-and-the-pacific/viet-nam/report-viet-nam/>.
- Amnesty International, *Vietnam: Let Us Breathe! Censorship and Criminalization of Online Expression in Vietnam*, (30 November 2020), available at: <https://www.amnesty.org/download/Documents/ASA4132432020ENGLISH.pdf>.
- Amnesty International, *Viet Nam: New Cybersecurity law a devastating blow for freedom of expression*, (12 June 2018), available at: <https://www.amnesty.org/en/latest/news/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression/>.
- Asia Indigenous Peoples Pact, *Indigenous Peoples' Statement – ASEAN People's Forum 2019*, (12 September 2019), available at: <https://aippnet.org/indigenous-peoples-statement-asean-peoples-forum-2019/>.
- Asia Sentinel, *Vietnam Tightens the Screws on the Internet*, Asia Sentinel, (4 May 2018), available at: <https://www.asiasentinel.com/p/vietnam-tightens-screws-internet>.
- CIVICUS, *People Power Under Attack 2020*, (2020), available at: <https://findings2020.monitor.civicus.org>.
- CIVICUS, Voice, Human Rights Foundation, *Socialist Republic of Vietnam Joint Submission to the UN Universal Periodic Review 32nd Session of the UPR Working Group*, (12 July 2018), available at: <https://civicus.org/documents/JointCIVICUSUPRSubmissionVietnam.pdf>.
- Circular No.38/2016/TT-BTTTT, (26 December 2016), available at: <https://vanbanphapluat.co/circular-38-2016-tt-btttt-specifying-cross-border-provision-public-information>
- Columbia University Global Freedom of Expression, *Public Prosecutor v. Nguyen Ngoc Nhu Quynh aka Mother Mushroom*, available at: <https://globalfreedomofexpression.columbia.edu/cases/public-prosecutor-v-nguyen-ngoc-nhu-quynh-aka-mother-mushroom/#:~:text=Nguyen%20Ngoc%20Nhu%20Quyn%20is,M%E1%BA%B9%20N%E1%BA%A5m%E2%80%9D%20or%20Mother%20Mushroom.&text=Nhu%20Quynh%20was%20arrested%20October,of%20the%20country%27s%20criminal%20code>.
- Criminal Code of 2015 (27 November 2015), available at: [https://www.policinglaw.info/assets/downloads/2015\\_Criminal\\_Code\\_of\\_Vietnam\\_\(English\\_translation\).pdf](https://www.policinglaw.info/assets/downloads/2015_Criminal_Code_of_Vietnam_(English_translation).pdf)
- Decree No.72/2013/ND-CP on the management, provision and use of Internet services and online information, (15 July 2013), available at: <https://vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF>
- Defend the Defenders, *Secret Trial Against Two Facebookers Huynh Anh Khoa and Nguyen Dang Thuong Suspended, New Date Rescheduled on December 21*, (7 December 2020), available at: <https://www.vietnamhumanrightsdefenders.net/2020/12/08/secret-trial-against-two-facebookers-huynh-anh-khoa-and-nguyen-dang-thuong-suspended-new-date-rescheduled-on-december-21/>.
- Defend the Defenders, *Vietnam Human Rights Defenders' Weekly Report for December 14-20, 2020: Activist Tran Duch Thach Convicted of Subversion, Sentenced to 12 years in Prison*, (20 December 2020), available at: <https://www.vietnamhumanrightsdefenders.net/2020/12/21/vietnam-human-rights-defenders-weekly-report-for-december-14-20-2020-activist-tran-duc-thach-convicted-of-subversion-sentenced-to-12-years-in-prison/>.
- Don Le, *New documentary series highlights the struggles of women activists in Vietnam*, Global Voices, (1 July 2019), available at: <https://globalvoices.org/2019/07/01/new-documentary-series-highlights-the-struggles-of-women-activists-in-vietnam/>.
- Elias Chachak, *Vietnam New Cyber Security Law, The Cyber Research Databank*, available at: <https://www.cyberdb.co/vietnam-new-cyber-security-law/#:~:text=According%20to%20a%202017%20report,being%20vulnerable%20to%20cyber%20attacks>.
- eQualitie, *News from Deflect Labs: DDoS attacks against Vietnamese Civil Society*, (7 September 2018), available at: <https://equalit.ie/ddos-attacks-vietnamese-civil-society/>
- Euan McKirdy, *'Stalinist' Vietnamese cybersecurity law takes effect, worrying rights groups and online campaigners*, CNN, (2 January 2019), available at: <https://edition.cnn.com/2019/01/02/asia/vietnam-cybersecurity-bill-intl/index.html>.
- Final Constitution of the Republic of Vietnam (28 November 2013), available at: <https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/94490/114946/F114201808/VNM94490%20Eng.pdf>.



FireEye, *Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations*, (14 May 2017), available at: <https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html>

Freedom House, *Freedom on the net 2020: Vietnam*, (2020), available at: <https://freedomhouse.org/country/vietnam/freedom-net/2020>.

Freedom House, *The Pandemic's Digital Shadow*, (2020), available at: <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>.

Frontline Defenders, *Digital Protection – More Safely Sharing, Communicating and Storing Digital Information*, available at: <https://www.frontlinedefenders.org/en/programme/digital-protection>.

Front Line Defenders, *Guide to Secure Group Chat and Conferencing Tools*, (30 August 2020), available at: <https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools>.

Frontline Defenders, *UPR Submission on Vietnam 32nd session*, (12 July 2018), available at: [https://www.frontlinedefenders.org/sites/default/files/fl\\_d\\_upr\\_32\\_vietnam\\_full.pdf](https://www.frontlinedefenders.org/sites/default/files/fl_d_upr_32_vietnam_full.pdf).

Giles Cooper and Hau Le, *Vietnam's new Cybersecurity Law: A headache in the making?*, Duane Morris, (July 2018), available at: [https://www.duanemorris.com/articles/static/cooper\\_le\\_cybersecurity\\_practitioner\\_0718.pdf](https://www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf).

Global Legal Group, *The International Comparative Legal Guide to: Telecoms, Media & Internet Law & Regulations 2018 11th Edition – A practical cross-border insight into telecoms, media and internet laws and regulations*, (2018), available at: [https://www.tilleke.com/sites/default/files/2017\\_Nov\\_ICLG\\_Telecoms\\_Vietnam.pdf](https://www.tilleke.com/sites/default/files/2017_Nov_ICLG_Telecoms_Vietnam.pdf).

Human Rights Committee, *Concluding observations on the third periodic report of Viet Nam*, CCPR/C/VNM/CO/3, (29 August 2019), available at: [https://tbinternet.ohchr.org/\\_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/VNM/CO/3&Lang=En](https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/VNM/CO/3&Lang=En)

Human Rights Committee, *Third periodic report submitted by Vietnam under Article 40 of the Covenant, due in 2004*, CCPR/C/VNM/3, (22 December 2017), available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/020/85/PDF/G1802085.pdf?OpenElement>

Human Rights Watch, *Vietnam: 6 Activists Headed to Prison*, (March 14, 2019), available at: <https://www.hrw.org/news/2019/03/14/vietnam-6-activists-headed-prison>.

Human Rights Watch, *Vietnam: Withdraw Problematic Cyber Security Law*, (7 June 2018), available at: <https://www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law>.

Hunter Marston, *Vietnam: why blogger Mother Mushroom went free*, The Interpreter, (24 October 2018), available at: <https://www.lowyinstitute.org/the-interpreter/vietnam-why-blogger-mother-mushroom-went-free>.

IFAD, AIPP, *Country Technical Note on Indigenous Peoples' Issues – Socialist Republic of Viet Nam*, (November 2012), available at: [https://www.ifad.org/documents/38714170/40224860/vietnam\\_ctn.pdf/c19c0ef7-ad08-4ef3-813f-4ce4c0fef407](https://www.ifad.org/documents/38714170/40224860/vietnam_ctn.pdf/c19c0ef7-ad08-4ef3-813f-4ce4c0fef407).

Ikigai Law, *Data protection in Vietnam*, (20 May 2020), available at: <https://www.ikigailaw.com/data-protection-in-vietnam/#acceptLicense>.

ILO Convention No.169, (1989), available at: [https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100\\_ILO\\_CODE:C169](https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C169)

Independent Advisory Group on Country Information, *Country Information and Guidance, Vietnam: Ethnic Minority Groups*, (December 2014), available at: [https://www.justice.gov/sites/default/files/pages/attachments/2015/06/19/cig.vietnam.ethnic\\_minority\\_groups.pdf](https://www.justice.gov/sites/default/files/pages/attachments/2015/06/19/cig.vietnam.ethnic_minority_groups.pdf).

Independent Advisory Group on Country Information, *Country Policy and Information Note Vietnam: Ethnic and religious groups*, (March 2018), available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/695864/Vietnam\\_-\\_Ethnic\\_and\\_Religious\\_groups\\_-\\_CPIN\\_v2.0\\_ex.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/695864/Vietnam_-_Ethnic_and_Religious_groups_-_CPIN_v2.0_ex.pdf).

International Commission of Jurists (ICJ), *Dictating the Internet: Curtailing Free Expression and Information Online in Vietnam*, (9 December 2020), available at: <https://www.icj.org/wp-content/uploads/2020/12/Vietnam-Freedom-of-expression-Publications-reports-thematic-reports-2020-ENG.pdf>.

International Commission of Jurists (ICJ), *Dictating the Internet: Curtailing Free Expression and Information Online in Southeast Asia*, (December 2019), available at: <https://www.icj.org/wp-content/uploads/2019/12/Southeast-Asia-Dictating-the-Internet-Publications-Reports-Thematic-reports-2019-ENG.pdf>.

International Covenant on Economic, Social and Economic Rights (ICESCR), available at: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>

International Covenant on Civil and Political Rights (ICCPR), available at: <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

International Federation for Human Rights (FIDH), *Vietnam Committee on Human Rights (VCHR), Joint Briefing paper on key human rights issues of concern*, (March 2019), available at: [https://queme.org/app/uploads/2019/03/FIDH-VCHR\\_EU-Vietnam-Dialogue\\_March\\_2019\\_EN.pdf](https://queme.org/app/uploads/2019/03/FIDH-VCHR_EU-Vietnam-Dialogue_March_2019_EN.pdf).

International Federation of Journalists, *Vietnam: Journalist Le Tuan arrested on anti-government propaganda charges*, (16 June 2020), available at: <https://www.ifj.org/media-centre/news/detail/category/press-releases/article/vietnam-journalist-le-tuan-arrested-on-anti-government-propaganda-charges.html>.

International Working Group for Indigenous Affairs (IWGIA), *Indigenous peoples in Vietnam*, (24 April 2019), available at: <https://www.iwgia.org/en/vietnam/3439-iw2019-vietnam.html>.

International Working Group for Indigenous Affairs (IWGIA) and AIPP, *Who We Are: Indigenous Peoples in Asia*, (2010), available at: [https://www.iwgia.org/images/publications/0640\\_ho\\_are\\_e\\_IPs\\_in\\_Asia.pdf](https://www.iwgia.org/images/publications/0640_ho_are_e_IPs_in_Asia.pdf).

Law on Access to Information, (6 April 2016), available at: <http://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=11040>

Law on Belief and Religion (18 November 2016), available at: <http://vbpl.vn/TW/Pages/vbpqen-toanvan.aspx?ItemID=11093>

Law on Cyberinformation Security No.86/2015/QH13 (19 November 2015), available at: <https://vanbanphapluat.co/law-no-86-2015-qb13-on-cyberinformation-security-2015>

Law on Cybersecurity 24/2018/QH14 (12 June 2018), available at: <https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf>

Law on Information Technology No.67/2006/QH11 (29 June 2006), available at: <https://vanbanphapluat.co/law-no-67-2006-qb11-of-june-29-2006-on-information-technology>

Law on National Security No.23/2004/QH11 (15 June 2004), available at: <https://vanbanphapluat.co/law-no-23-2004-qb11-of-june-15-2004-on-inland-waterway-navigation>

Law on Telecommunications No.41/2009/QH12 (23 November 2009), available at: <https://vanbanphapluat.co/law-no-41-2009-qb12-on-telecommunications>

Law on the Protection of State Secrets (29 November 2018), available at: <https://english.luatvietnam.vn/aw-no-29-2018-qb14-of-the-national-assembly-on-protection-of-state-secrets-169341-Doc1.html>

Manushya Foundation, *Are We Free Online? – Digital Rights in Vietnam*, (15 October 2020), available at: <https://www.manushyafoundation.org/post/are-we-free-online-digital-rights-in-vietnam>.

Manushya Foundation, *#StopDigitalDictatorship in Southeast Asia*, available at: <https://www.manushyafoundation.org/stop-digital-dictatorship-campaign>.

Minority Rights Group International, *World Directory of Minorities and Indigenous Peoples – Vietnam: Highlanders*, (March 2018), available at: <https://www.refworld.org/docid/49749c7e16.html>.

Nhân Dân, *Law on protection of state secrets approved*, (15 November 2018), available at: <https://en.nhandan.org.vn/politics/item/6844702-law-on-protection-of-state-secrets-approved.html>.

Pen America, *Poet and Writer Tran Duc Thach Sentenced to 12 Years in Vietnamese Prison*, (17 December 2020), available at: <https://pen.org/press-release/poet-and-writer-tran-duc-thach-sentenced-to-12-years-in-vietnamese-prison/>.

Press Law No.103/2016/QH13 (5 April 2016), available at: <https://vanbanphapluat.co/law-103-2016-qb13-press>

Radio Free Asia (RFA), *Dissent Vietnamese Poet Jailed for 12 years on ‘Subversion’ Charge*, (15 December 2020),

available at: <https://www.rfa.org/english/news/vietnam/jailed-12152020145411.html>.

Radio Free Asia (RFA), *Vietnam Arrests Journalists for Tollbooth Scheme Criticism*, (17 December 2020), available at: <https://www.rfa.org/english/news/vietnam/bot-12172020164523.html>.

Radio Free Asia (RFA), *Vietnamese Court Indicts Leaders of Independent Journalists Association*, (11 November 2020), available at: <https://www.rfa.org/english/news/vietnam/ijavn-11112020194743.html>.

Reporters Sans Frontières, *RSF dénonce la condamnation à vingt ans de prison du blogueur vietnamien Le Dinh Luong*, (6 March 2019), available at: <https://rsf.org/fr/actualites/rsf-denonce-la-condamnation-vingt-ans-de-prison-du-blogueur-vietnamien-le-dinh-luong>.

Reuters, *Vietnam steps up online crackdown, jailed activists at record high – Amnesty*, (30 November 2020), available at: <https://in.reuters.com/article/vietnam-security-socialmedia/corrected-vietnam-steps-up-online-crackdown-jailed-activists-at-record-high-amnesty-idINL4N2IG2LN>.

Rights Con, Manushya Foundation, PEN International, *Will democracy survive ‘national security’ in the digital space of Southeast Asia*, (2020), available at: [https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76\\_3cd3d0295715413f8acfa25a933d482.pdf](https://a9e7bfc1-cab8-4cb9-9c9e-dc0cee58a9bd.filesusr.com/ugd/a0db76_3cd3d0295715413f8acfa25a933d482.pdf).

The 88 Project, *Vietnam Free Expression Newsletter No.37/2020 – Week of September 14-20*, (21 September 2020), available at: <https://the88project.org/newsletter-no-37/>.

The 88 Project, *Vietnam Human Rights Report, January – June 2019: Crackdown on Facebook Users, Civil Society Groups, and Public Protestors Continues*, (31 July 2019), available at: <https://the88project.org/vietnam-human-rights-report-january-june-2019-crackdown-on-facebook-users-civil-society-groups-and-public-protestors-continues/>.

The Advocates for Human Rights, Tai Studies Center, *VIETNAM Submission to the Human Rights Committee RELATING TO THE RIGHTS OF INDIGENOUS PEOPLES*, (4 February 2019), available at: [https://www.theadvocatesforhumanrights.org/uploads/vietnam\\_ahr\\_tsc\\_iccpr\\_shadow\\_report\\_submitted\\_3.pdf](https://www.theadvocatesforhumanrights.org/uploads/vietnam_ahr_tsc_iccpr_shadow_report_submitted_3.pdf).

Thoi Bao.De, *Truong Chau Huu Danh arrested: A lawyer said Article 331 is “ambiguous”*, (20 December 2020), available at: <https://thoibao.de/blog/2020/12/20/truong-chau-huu-danh-arrested-a-lawyer-said-article-331-is-ambiguous/>.

Tuoi Tre News, *Vietnam police arrest Truong Chau Huu Danh for abusing rights to free speech, press freedom*, (17 December, 2020), available at: <https://tuoitrenews.vn/news/society/20201217/vietnam-police-arrest-truong-chau-huu-danh-for-abusing-rights-to-free-speech-press-freedom/58335.html>.

United Nations Declaration on the Rights of the Indigenous Peoples, available at: [https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP\\_E\\_web.pdf](https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf)

Universal Declaration on Human Rights, available at: <https://www.un.org/en/universal-declaration-human-rights/>

Universal Declaration on Human Rights Defenders, available at: <https://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx>

Unrepresented Nations and Peoples Organization, *Alternative Report submitted to the UN Committee on the Elimination of Racial Discrimination at the 80th Session during the consideration of the 10th to 14th Periodic Reports of the Socialist Republic of Viet Nam*, (January 2012), available at: <https://unpo.org/downloads/1734.pdf>.

U.S Commission on International Religious Freedom, *Vietnam Tier 1 – USCIRG Recommended Countries of Particular Concern (CPC)*, (2019), available at: <https://www.justice.gov/eoir/page/file/1158891/download#:~:text=On%20January%201%2C%202018%2C%20Vietnam%27s,a%20right%20to%20legal%20personhood>.

U.S Department of State, *Vietnam 2019 Human Rights Report*, (2019), available at: <https://www.state.gov/wp-content/uploads/2020/03/VIETNAM-2019-HUMAN-RIGHTS-REPORT.pdf>.

Vietnam Committee on Human Rights, *Violations of the Rights of Ethnic and Religious Minorities in the Socialist Republic of Vietnam*, (January 2012), available at: [https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/VNM/INT\\_CERD\\_NGO\\_VNM\\_80\\_10313\\_E.pdf](https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/VNM/INT_CERD_NGO_VNM_80_10313_E.pdf).

Vietnam Human Rights Defenders, *Vietnam's 'Cybersecurity' Law Says Little on Security*, Defend The Defenders, (January 2019), available at: <https://www.vietnamhumanrightsdefenders.net/2019/01/12/vietnams-cybersecurity-law-says-little-on-security/>.

Vietnam Law & Legal Forum, *New Law on Access to Information*, (7 November 2016), available at: <https://vietnamlawmagazine.vn/new-law-on-access-to-information-5598.html>.





IEHRDs and the communities they work with have often become particular targets of the governments as they mostly challenge the laws, policies and practices related to lands and resources, which contrasts with the State aspiration to control them as well as business interests over them. In lack of legal recognition of or respect for the rights of Indigenous communities as well as strong push for economic growth in the Mekong countries, the communities and their supporting IEHRDs are caught up in land and resource conflicts with the State and business entities. During the course of the legitimate resistance to defend human and environmental rights, IEHRDs encounter a series of challenges for their works as well as face risks and reprisals. Those challenges and reprisals often begin with social stigmatization against the IEHRDs as “anti-development” and “anti-national” and include harassment, threats, attacks, arbitrary arrests and detentions, prosecution and even enforced disappearances and killings of the IEHRDs.