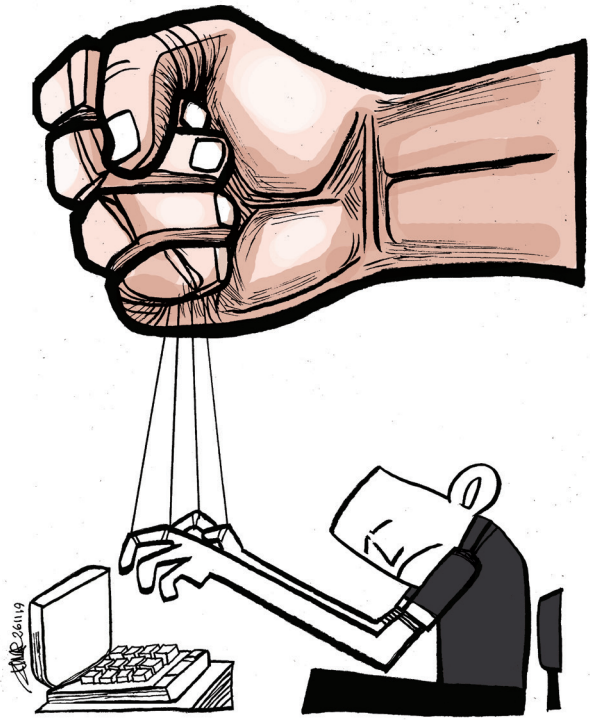
Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia



International Commission of Jurists

Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia

Composed of 60 eminent judges and lawyers from all regions of the world, the International Commission of Jurists (ICJ) promotes and protects human rights through the Rule of Law, by using its unique legal expertise to develop and strengthen national and international justice systems.

Established in 1952 and active on the five continents, the ICJ aims to ensure the progressive development and effective implementation of international human rights and international humanitarian law; secure the realization of civil, cultural, economic, political and social rights; safeguard the separation of powers; and guarantee the independence of the judiciary and legal profession.

® Dictating the Internet: Curtailing free expression, opinion and information online in Southeast Asia

Published in December 2019

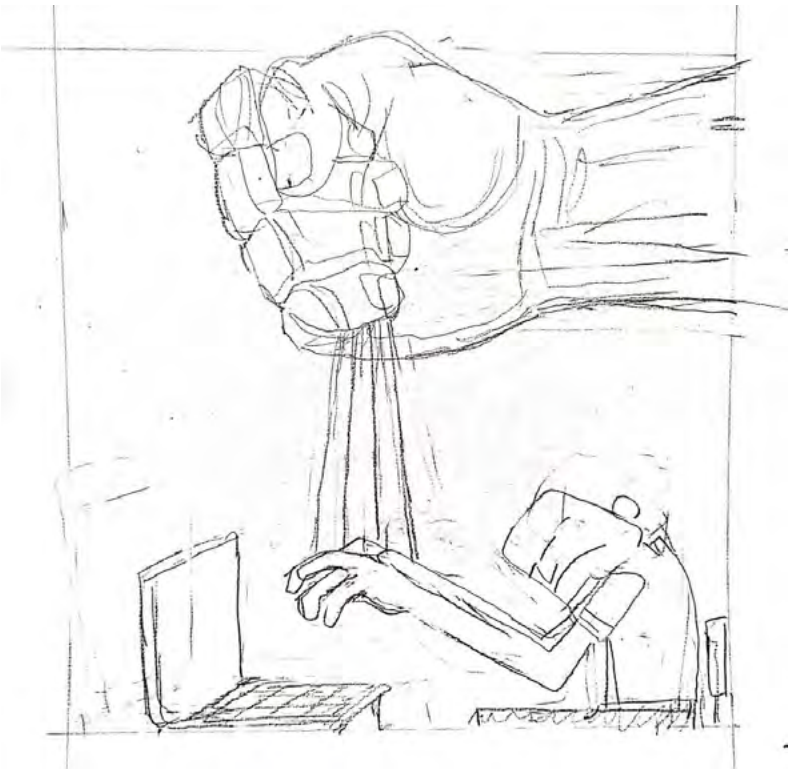
International Commission of Jurists

P.O. Box 91 Rue des Bains 33

Geneva

Switzerland

Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia



This report was researched and drafted by Dhevy Sivaprakasam.

Legal review and direction were provided by Frederick Rawski and Ian Seiderman.

Sanhawan Srisod, Sean Bain, Michelle Yesudas, Jenny Domino and Ruth Stephani Panjaitan also provided input that informed this report.

The cartoons included in this report were drawn by Zunar.

The ICJ would like to acknowledge the following organizations, whose information and analyses were referenced in this report:

Access Now

Advocates' Association of Sarawak

Amnesty International

Article 19

Asia Internet Coalition

Association for Progressive Communications

Athan Myanmar

BSA The Software Alliance

Cambodian Center for Human Rights

Cambodian League for the Promotion and Defense of Human Rights (LICADHO)

Cross-Cultural Foundation

Defend the Defenders

Free Expression Myanmar

Frontline Defenders

Human Rights Foundation Center for Law and Democracy

Human Rights Watch

iLaw

International Federation for Human Rights (FIDH)

Lao Movement for Human Rights

Lawyers for Liberty

Malaysian Bar Association

Manushya Foundation

Political Prisoners in Thailand

Reporters Sans Frontières

Sabah Law Association

Southeast Asian Press Alliance

Thai Lawyers for Human Rights

Thai Netizen Network

The 88 Project

The Brunei Project

And all other partners – individuals and organizations – who provided input that informed this report.

TABLE OF CONTENTS

Executive Summary

The internet is the world's most powerful medium of communication. For most of the world's population, it is a significant means of exercising the rights to freedom of expression, opinion and information, and for participating in public life.

The internet can, however, serve as a double-edged sword. People now enjoy unprecedented access to information. At the same time, the spread of hate speech, incitement to violence, disinformation or propaganda and risks of cyber-attacks on State and other organizational infrastructure pose threats not only to the exercise of the rights to freedom of expression, opinion and information, but also to privacy, religious freedom and belief, and public participation, among other rights.

These challenges demand genuine law and policy responses. In Southeast Asia, however, legislation and regulatory action introduced by States ostensibly to address these challenges has instead been used to suppress speech and target critics in violation of human rights law obligations and in a manner that undermines the rule of law.

Through analyses of legal frameworks and selected cases throughout the region[1], this report maps out a general pattern of abuse across the region, where legal provisions have been implemented in a way that curtails the rights to freedom of expression, opinion and information online.

This trend is not new – Southeast Asian governments have, for decades, crafted and enforced the law to curtail expression and information, and have in recent years extended these old patterns of violation to the online sphere.

Laws enacted before the internet era – including those prohibiting defamation, lesè majesté, sedition, contempt of court or crimes against the State – have been repurposed or supplemented to censor expression and information online. More recent laws that have been introduced purportedly to regulate information online, control the spread of disinformation, ensure cybersecurity and justify internet shutdowns have been used for the same aims.

1 The information in this report is accurate as of 26 November 2019.

These frameworks commonly include vague, overbroad legal provisions; severe and disproportionate penalties; lack independent oversight mechanisms; and fail to provide effective remedy or accountability. Conceptions of "national security" and "public order" have been conflated with the perceived interests of the ruling government or other powerful interests to target specific expression.

Emerging laws allow for extraterritorial application, and in some cases, seek to extend their reach beyond public expression, to private communications. These frameworks do not advance legitimate aims in accordance with the principles of legitimacy, necessity and proportionality required by the rule of law, in violation of international law.

This report concludes by reasserting that international human rights law not only remains relevant, but that its application is needed, now more than ever in the digital age, to protect the exercise of rights online as well as offline.

It calls for States in Southeast Asia to repeal, amend or otherwise rectify existing legal and regulatory frameworks to bring them in line with their international obligations. The report argues that respect for human rights is essential not only for ensuring that all members of the global community can fully enjoy and exercise their freedom of expression, opinion and information, but that legislation framed in human rights terms is also the best and most effective way to protect against the very real threats posed by the spread of hate speech, disinformation online, cyber-attacks and other cybercrimes.

Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia

This report analyzes how governments in Southeast Asia have used the law to restrict and control expression and content online to the detriment of individuals' rights to freedom of expression and information. For decades, laws which establish defamation, lesè majesté, sedition, contempt of court or "crimes against the State" as criminal offences have been promulgated and invoked to protect national security and ensure public order. In reality, States have conflated "national security" with the perceived interests of the government or other powerful interests and targeted a range of views, including critical dissent, expressed by individuals both offline and online. "Public order" has also been used as a justification to violate individuals' rights to expression, information, privacy, bodily integrity and security. This trend of abuse continues, and in recent years has expanded to the online sphere, through the enforcement of a new generation of laws that purportedly aim to regulate information online, control the spread of disinformation online, ensure cybersecurity and sometimes permit internet shutdowns, typically on the basis of ensuring public order.

The ICJ acknowledges that the spread of content that serves to harm the rights or reputations of others, including hate speech or incitement to violence online, and "cyber-attacks" are serious problems which require urgent law and policy solutions.[2] In Southeast Asia, however, legislative attempts by governments to combat these challenges appear generally not to have been introduced in good faith, and certainly not in a manner consistent with human rights and the rule of law. The ICJ intends for this report to contribute to human rights-compliant policy solutions by documenting past abuses and identifying problematic aspects of existing legal frameworks with the aim of contributing in a positive and constructive manner to efforts to develop new legal frameworks that address the human rights and rule of law challenges and opportunities that new technologies bring.

2 This includes defamatory content, the spread of private personal content without consent of the owner of such content, disinformation or propaganda, within the context of elections for example, that can negatively impact upon an individual's ability to exercise his or her other rights, such as the right to privacy, the right to vote or the rights to hold opinions without interference and to seek, receive and impart information.

I. Background

The internet is the world's most powerful medium of communication. For much of the world's population, it is a primary means of receiving and sending communication at a distance and participating in public life. People exercise their human rights and fundamental freedoms as much online as they do offline.[3] As of April 2019, 58 percent of the world's population were using the internet and 45 percent were active users of social media platforms.[4] As more and more people turn to online platforms to exercise their rights to freedom of expression, opinion and information, it is essential that States discharge their obligations to protect and fulfil human rights in the online sphere.[5] This includes taking steps to regulate the conduct of certain private actors, such as telecommunications providers and social media platforms, that mediate and regulate digital access and information flows online. These private companies themselves must also respect and protect these rights.

From a human rights perspective, the internet can serve as a double-edged sword. People now enjoy unprecedented access to information and a powerful new means to exercise freedom of expression. At the same time, abusive expression in the form of hate speech or information inciting violence and the spread of disinformation[6] or propaganda[7] (which can interfere with the rights to information, opinion and privacy) have increased, in ways that

3 Miniwatts Marketing Group, 'Internet Growth Statistics', 9 May 2019, Available at: https://www.internetworldstats.com/emarketing.htm; UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35, para 1.

4 International Telecommunications Union, 'ITU releases 2018 global and regional ICT estimates', 7 December 2018, Available at: https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx; Simon Kemp, 'The State of Digital in 2019: All the Numbers You Need to Know', *We Are Social*, 25 April 2019, Available at: https://wearesocial.com/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know

5 See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 30 March 2017, A/HRC/35/22 ('A/HRC/35/22'), paras 1, 3; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018, A/HRC/38/35 ('A/HRC/38/35'), para 1.

6 This paper adopts the definition of "disinformation" as "false information knowingly shared to cause harm", in contrast with "misinformation" as when "false information is shared, but no harm is meant". This is the categorization put forth by Wardle and Derakhshan, which was adopted by a study commissioned by the European Parliament on the impact of disinformation and strategic political propaganda disseminated through online social media sites on the functioning of the rule of law, democracy and fundamental rights. See Policy Department for Citizens' Rights and Constitutional Affairs, 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States', February 2019 ('European Parliament, February 2019'), p. 26, Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf, referring to Wardle, C. and Derakhshan H., 'Information disorder: Toward an interdisciplinary framework', Council of Europe, 2017, p.21.

7 This report notes that "propaganda" can generally be defined as the "art of influencing, manipulating, controlling, promoting, changing, inducing, or securing the acceptance of opinions, attitudes, action, or behaviour", as observed by European Parliament, February 2019, p. 26, referring to Martin, J., 'Definition of propaganda in "International Propaganda: Its Legal and Diplomatic Control"', University of Minnesota Press, 1958, p. 10.

are difficult to regulate. In some cases, they should not be the subject of regulation.[8] Moreover, use of the internet exposes users to violations and abuses of their rights, including the rights to privacy and security, whether through surveillance by State authorities or the use of personal data by companies for commercial purposes. Cyber-attacks on State and other organizational online infrastructure also demand a genuine law and policy response. These problems pose threats to the exercise of the rights to freedom of expression, opinion and information, privacy, religious freedom and belief, and public participation, among other rights.[9]

In Southeast Asia, these problems are particularly acute due to a variety of factors. The region has more than 400 million internet users.[10] At the same time, there are enormous disparities across and within countries when it comes to access to social media. Access to the internet has exposed previously isolated communities to the full weight of the global media eco-system with little preparation. In some cases, this has happened over a period of just a few years. The region also has a diverse range of governance regimes, including authoritarian States that exercise near total control over public discourse. Many of these governments have been unprepared for the profound impact that internet access has had on their ability to control their populations and suppress public expression, which may include speech that is critical of State authorities. This has led to a proliferation of laws ostensibly meant to address issues of legitimate concern, such as hate speech, defamation, electoral security and cybersecurity, but which have more often been used to target critics and constrain civic space.

The rise of internet-based communications and social media have exacerbated existing social tensions, and provided new tools for powerful State and non-State actors to exploit and introduced new vulnerabilities for civil society, judiciaries and other institutions that require open discourse

8 In a 2017 joint declaration, the UN Special Rapporteur on freedom of expression and three regional rapporteurs with equivalent mandates noted that "disinformation and propaganda are often designed and implemented so as to mislead a population, as well as to interfere with the public's right to know and the right of individuals to seek and receive, as well as to impart, information and ideas of all kinds", and "some forms of disinformation and propaganda may harm individual reputations and privacy, or incite to violence, discrimination or hostility against identifiable groups in society". See the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda', 3 March 2017, Available at: https://www.osce.org/fom/302796?download=true

9 A/HRC/38/35, para 5.

10 ASEAN UP, 'Southeast Asia digital, social and mobile 2019', 31 July 2019, Available at: https://aseanup.com/southeast-asia-digital-social-mobile/

and freedom from political manipulation in order to effectively operate. These include the role of social media in spreading unprotected hate speech, particularly that which incites violence, manipulation of elections and other democratic processes through the spread of disinformation, and a new generation of security concerns associated with cyberspace.

In Myanmar, the proliferation of hate speech on social media platforms has contributed to discrimination and violence against ethnic and religious minorities. In 2018, the UN Independent International Fact-Finding Mission on Myanmar found that "extreme violence" against and "marginalizing and othering" of the Rohingya minority group had been facilitated by "concerted hate campaigns with the involvement of and condoning by State authorities", which had been "greatly facilitated by social media platforms."[11] Similarly, the UN Special Rapporteur on the situation of human rights in Myanmar warned that Facebook had "turned into a beast", enabling the proliferation of incitement to violence and hatred on its platform.[12] In the same year, a Reuters report found that language barriers and insufficient resources and attention dedicated by Facebook to address these barriers had made this proliferation possible, and that Facebook was not the only social media platform facing these challenges.[13] Hate speech is a pressing concern for which both legal and technical responses need to be developed. Unfortunately, as set out in this report, efforts that have been introduced by the governments to date seem more tailored to suppressing free expression that is politically unwelcome than countering attacks and incitement against minorities.

In Indonesia, the spread of disinformation online before and during elections has threatened to delegitimize the election process and exacerbate

11 Statement of Mr. Marzuki Darusman, Chairperson of the Independent International Fact-Finding Mission on Myanmar to the General Assembly, Third Committee, 23 October 2018. Available at: https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=23800&LangID=E; Darusman further stated that Facebook "substantively contributed to the level of acrimony and dissension and conflict… within the public. Hate speech is certainly of course a part of that." See Tom Miles, 'U.N. investigators cite Facebook role in Myanmar crisis', *Reuters,* 13 March 2018, Available at: https://uk.reuters.com/article/us-myanmar-rohingya-facebook/u-n-investigators-cite-facebook-role-in-myanmar-crisis-idUKKCN1GO2PN

12 BBC, 'UN: Facebook has turned into a beast in Myanmar', 13 March 2018. Available at: https://www.bbc.com/news/technology-43385677; Report of the Special Rapporteur on the situation of human rights in Myanmar, 5 March 2019, A/HRC/40/68, paras 54, 55; Notably, incitement to violence and hatred on Facebook targeting Rohingya Muslims who had sought refuge in India was also a "big problem" outside of Myanmar. See Vindu Goel, Shaikh Azizur Rahman, 'When Rohingya Refugees Fled to India, Hate on Facebook Followed', *New York Times,* 14 June 2019, Available at: https://www.nytimes.com/2019/06/14/technology/facebook-hate-speech-rohingya-india.html?te=1&nl=morning-briefing&emc=edit_MBAE_p_20190616&section=whatElse?campaign_id=7&instance_id=10252&segment_id=14352&user_id=3f72f2845ba8594bb0e4459957511f9b&regi_id=87913927ion=whatElse

13 Steve Stecklow, 'Inside Facebook's Myanmar operation: Hatebook - A Reuters Special Report' Reuters, 15 August 2018, Available at: https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/

identity-based political polarization. In 2017, prior to Jakarta's gubernatorial elections, then governor Basuki Tjahaja Purnama, an ethnic Chinese Christian, was convicted of blasphemy and sentenced to two years' imprisonment after a doctored video circulated online which misrepresented comments that he made suggesting that certain Quranic verses had been inappropriately invoked to discourage Muslims from voting for him.[14] The maker of the video was only held accountable after Purnama lost the elections and completed his prison term.[15] Prior to Indonesia's 2019 general elections, the spread of disinformation again posed serious problems. Between December 2018 and January 2019, the civil society organization MAFINDO reported that online disinformation had increased by 61 percent, with nearly half of such false information being shared on Facebook.[16]

In Singapore, breaches of cybersecurity exposed confidential information which infringed upon the privacy rights of individuals and heightened potential risks of violation of other rights. Between June and July 2018, a cyber-attack on Singapore's largest group of healthcare institutions led to breach of privacy and stealing of confidential data from some one-and-a-half million patients.[17] In January 2019, the Ministry of Health's HIV Registry was hacked and the confidential information of 14,200 HIV-positive individuals was leaked – exposing a vulnerable community to increased risk of discrimination, particularly with respect to the exercise of their rights to health, work and social security.[18]

The threat of cyber-attacks and the proliferation of disinformation and hate speech online are real problems, requiring urgent policy solutions. The ICJ believes that such policies will be greatly improved if they are human rights-compliant, frame these issues as human rights concerns, and employ analytical tools and accountability mechanisms that an international law

14 Asian Correspondent, 'Ahok release an uncomfortable reminder of the power of blasphemy laws', 24 January 2019, Available at: https://asiancorrespondent.com/2019/01/ahoks-release-an-uncomfortable-reminder-of-the-power-of-blasphemy-laws/

15 *Ibid.*

16 Kate Lamb, 'Fake news spikes in Indonesia ahead of elections', *The Guardian,* 20 March 2019, Available at: https://www.theguardian.com/world/2019/mar/20/fake-news-spikes-in-indonesia-ahead-of-elections. MAFINDO – Masyarakat Anti Fitnah Indonesia – began as a grassroots movement, leading efforts to combat fake news online. See https://www.mafindo.or.id/about/.

17 Irene Tham, 'Top-secret report on SingHealth attack submitted to Minister-in-charge of Cyber Security', *Straits Times*, 31 December 2018, Available at: https://www.straitstimes.com/singapore/top-secret-report-on-singhealth-attack-submitted-to-minister-in-charge-of-cyber-security

18 Salma Khalik, 'Data of 14,200 people with HIV leaked online by US fraudster who was deported from Singapore', *Straits Times*, 28 January 2019, Available at: https://www.straitstimes.com/singapore/data-of-14200-singapore-patients-with-hiv-leaked-online-by-american-fraudster-who-was; Sharanjit Leyl, 'Singapore HIV data leak shakes a vulnerable community', *BBC*, 22 February 2019, Available at: https://www.bbc.com/news/world-asia-47288219

approach can provide. While this report focuses on Southeast Asia, these issues are clearly of global concern, and many will require solutions at a global level.[19]

***

This report begins by explaining how governments in Southeast Asia have historically used laws and legal frameworks to censor or otherwise regulate content and define what constitutes "legitimate" expression online primarily for political reasons, including preservation of their own power and authority. Importantly, legislative efforts by governments within the region have bolstered and reinforced similar efforts by their neighbours. This trend to exercise greater controls over online speech is in many cases a natural evolution from past attempts to suppress critical voices, and can be addressed with many of the same law and advocacy tools used by human rights defenders in the past. In other cases, new technologies have transformed the conversation in a more dramatic way – such as the introduction of more comprehensive legal regimes regulating cybersecurity and online communications – and may require more creative legal and technological responses.

Southeast Asia has consistently been ranked as one of the weakest regions in the world in protecting the rights to free expression, opinion and information. In 2019, a report by international non-governmental organization on media freedoms, Reporters Sans Frontières, ranked Southeast Asia in the bottom third of the World Press Freedom Index,[20] and noted that six of the ten States had declined in media freedom from 2018.[21] The regional backslide in rights protection has only intensified in recent years, with governments targeting expression and information online by introducing repressive laws justified by the need to combat online hate speech, disinformation and cyber-attacks.

19 The UN Special Rapporteur on freedom of expression highlighted that the restriction of free expression online was a "global phenomenon". See Al Jazeera, 'UN investigator David Kaye: Break up Facebook, Google', 9 June 2019, Available at: https://www.aljazeera.com/programmes/talktojazeera/2019/06/special-rapporteur-freedom-speech-190608101807323.html

20 Southeast Asia has consistently fallen in the bottom third of rankings since RSF's annual publishing of the World Press Freedom Index began in 2002. See RSF, 'The World Press Freedom Index', Available at: https://rsf.org/en/world-press-freedom-index

21 Southeast Asian Press Alliance, '[Regional] Journalist safety declines as authoritarian regimes tighten grip on media —RSF', 18 April 2019, Available at: https://www.seapa.org/regional-journalist-safety-declines-as-authoritarian-regimes-tighten-grip-on-media-rsf/

These developments are part of a global trend. In 2019, the United Nations Special Rapporteur on freedom of expression highlighted a "global phenomenon" of increasing interference by States with free expression, opinion and information online.[22] In 2019, a report by data and risk analytics company Verisk Maplecroft highlighted a "rising tendency for governments to adopt more extreme measures to protect their own interests" with respect to matters such as data privacy, mass surveillance and attacks against journalists and activists, and classified approximately 45 percent of the global population as living in 58 countries where the rights to freedom of expression, information and privacy were at 'extreme risk'.[23]

The crucial role of social media platforms and the accompanying struggle between governments and private ICT sector companies for control of information on these platforms is also a key factor that will inform this paper's analysis. States are increasingly co-opting social media platforms. In 2019, a report by the Oxford Internet Institute found that manipulation of social media towards political purposes had been employed in 70 countries, a jump from 48 countries in 2018 and 28 countries in 2017 – with Facebook often being the targeted medium for manipulation.[24] It also found that, in 26 countries, social media had been manipulated to "suppress fundamental human rights, discredit political opponents, and drown out dissenting opinions".[25] Meanwhile, States are also attempting to regulate and control dissemination of information on social media platforms. In October 2019, the European Court of Justice delivered a verdict enabling European Union member states to force Facebook to take down content deemed illegal under domestic law – such as defamatory content – not only domestically but also globally across its platform – raising concerns about the impact of this judgment on free speech online.[26]

22 See footnote 19; In a report released in November 2019, Freedom House noted that 33 of 65 assessed countries had observed a decline in internet freedoms since June 2018, See Adrian Shahbaz, Allie Funk, 'Freedom on the Net 2019: The Crisis of Social Media', Available at: https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media

23 Sofia Nazalya, "Strongmen' regimes lead charge against freedom of speech and privacy: Human Rights Outlook 2019', 7 August 2019, Available at: https://www.maplecroft.com/insights/analysis/strongmen-regimes-lead-charge-against-freedom-of-speech-and-privacy/

24 Bradshaw, S. and Howard, P.N., 'The Global Disinformation Order 2019 Global Inventory of Organised Social Media Manipulation', Oxford Internet Institute, Computational Propaganda Research Project, 2019 ('Bradshaw and Howard, 2019') p. 2. The report noted, in its Introduction, "Around the world, government actors are using social media to manufacture consensus, automate suppression, and undermine trust in the liberal international order. … The use of computational propaganda to shape public attitudes via social media has become mainstream, extending far beyond the actions of a few bad actors. In an information environment characterized by high volumes of information and limited levels of user attention and trust, the tools and techniques of computational propaganda are becoming a common – and arguably essential – part of digital campaigning and public diplomacy."

25 Bradshaw and Howard, 2019, p.5. These countries included Cambodia, Thailand and Vietnam.

26 Adam Satariano, 'Facebook Can Be Forced to Delete Content Worldwide, E.U.'s Top Court Rules',

The legal trends and emblematic cases highlighted in this paper and the recommendations offered to address related human rights abuses should therefore have relevance beyond the region.

***

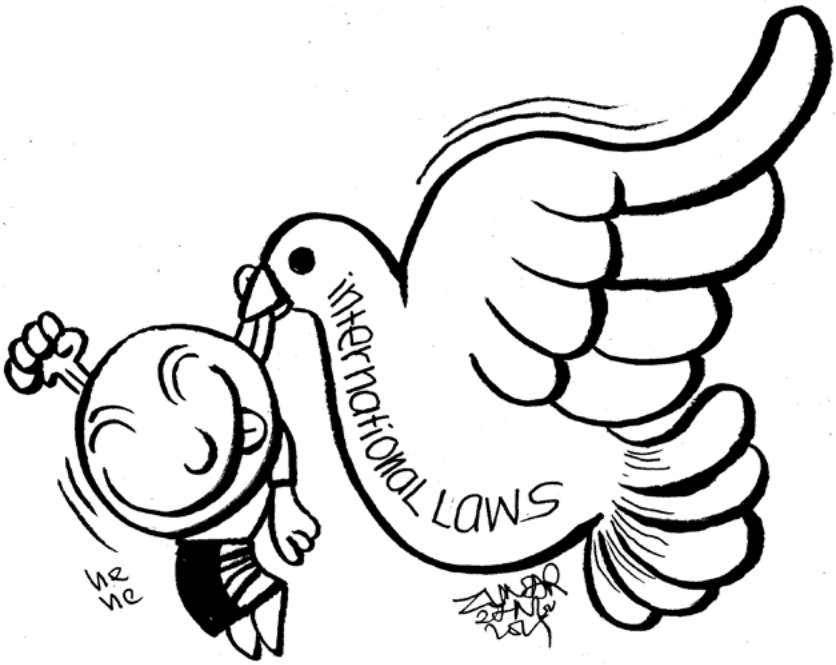
New York Times, 3 October 2019, Available at: https://www.nytimes.com/2019/10/03/technology/facebook-europe.html; While this judgment crucially held that national courts are obliged to ensure their decisions are in line with international law, how it will be enforced in practice raises concerns that this judgment may negatively impact on freedom of expression and information online, particularly with respect to extraterritorial application on information shared between jurisdictions. Similar concerns are engaged by laws promulgated in Southeast Asia which allow for extraterritorial application such as Singapore's Protection from Online Falsehoods and Manipulation Act.

II. International law and standards

The international human rights framework governing the rights to freedom of expression, opinion and information anchors the analysis in this report of an existing and emerging generation of laws regulating information and communications technologies (ICT). As will be evident in this paper, the underlying human rights concerns presented by these laws are not fundamentally different from those implicated by previous efforts to suppress offline speech, and in fact merely extend old patterns of violation to the online sphere.

This section begins by providing a brief overview of those human rights laws and principles, expressed in article 19 of the UN Declaration of Human Rights (UDHR) and, as a legal treaty obligation, in article 19 of the International Covenant on Civil and Political Rights (ICCPR) and customary international law. It then considers developments at the international level to address issues that arise in the context of online expression, including their impacts on the rights to freedom of association and assembly, political participation and privacy.

This report does not contain a targeted analysis of impacts on the right to privacy by ICT-regulating laws. Nonetheless, the right to privacy is crucially engaged and must be considered within this context. This section thus also provides a summary of the right to privacy as defined under international law and standards.


International Laws

i. The right to freedom of expression, opinion and information

International law protects the right of every individual to freedom of opinion and expression, including the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers, under article 19 of ICCPR and article 19 of the UDHR, generally considered to reflect customary international law in this area. It is also protected in regional human rights treaties, including the American Convention on Human Rights, the African Charter on Human and Peoples Rights, the Arab Charter on Human Rights and the European Convention of Human Rights.

The great majority of States, albeit not all in the Southeast Asia, have assumed particular legal obligations to respect and protect these rights which enjoy universal protection as general rights protected under the ICCPR.[27] Irrespective of whether States are party to the ICCPR, however, these rights must be protected under customary international law. States, including States in Southeast Asia, have reaffirmed this commitment in numerous declaratory statements and UN and other intergovernmental resolutions. For instance, the Vienna Declaration and Programme of Action adopted by consensus of all UN member states at the World Conference on Human Rights in 1993 reaffirmed the "commitment of *all* States to fulfil their obligations to promote universal respect for, and observance and protection of, all human rights and fundamental freedoms in accordance with … instruments relating to human rights, and international law", including the right to freedom of expression.[28]

Article 19 of the ICCPR specifically provides that:

"1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to

27 Cambodia, Indonesia, Laos, Philippines, Thailand and Vietnam have ratified or acceded to the ICCPR, while Brunei Darussalam, Malaysia, Myanmar and Singapore have not.

28 Emphasis by author. Vienna Declaration and Programme of Action, 25 June 1993, Available at: https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx

certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals."

The UN Human Rights Committee, mandated under the ICCPR to supervise its implementation and interpret its provisions has clarified that freedom of expression and opinion are "indispensable conditions" for the advancement of any person or society.[29] These rights are intertwined, as freedom of expression and information facilitates the evolution and exchange of opinions, in turn enabling "principles of transparency and accountability" crucial for the promotion and protection of human rights.[30] They also are related to the enjoyment of other rights in general, including the "rights to freedom of assembly and association, and the exercise of the right to vote".[31]

The UN Human Rights Committee has clarified that protections for freedom of expression and opinion should extend to "political discourse, commentary… on public affairs, canvassing, discussion of human rights, journalism… and religious discourse", including through non-verbal means and "electronic and internet-based modes of expression".[32] It has further noted that "developments in internet and mobile based electronic information dissemination systems" have established a "global network" for information exchange where States should take steps to ensure that media broadcasting services can function independently and are accessible to individuals.[33] In this respect, the Committee has affirmed the crucial function of independent, uncensored media to ensure "free communication of information and ideas… between citizens, candidates and elected representatives" and to "inform public opinion".[34]

The obligation of every State to respect and protect the rights to free expression, opinion and information must be upheld by all branches of the State – executive, legislative and judicial – and other public or governmental bodies. It also extends to protection for individuals from

29 UN Human Rights Committee, General Comment No. 34, CCPR/C/GC/34, 12 September 2011 ('CCPR/C/GC/34'), para 2.
30 CCPR/C/GC/34, paras 2, 3.
31 CCPR/C/GC/34, para 4.
32 CCPR/C/GC/34, para 11.
33 CCPR/C/GC/34, paras 15, 16.
34 CCPR/C/GC/34, para 13.

"any acts by private persons or entities that would impair the enjoyment of the freedoms … to the extent (they) are amenable to application between private persons or entities".[35] This obligation further entails that these rights are protected under domestic law, including provision for remedies when the rights are violated.[36]

In this respect, "harassment, intimidation or stigmatization of a person, including arrest, detention, trial or imprisonment" solely for the exercise of the right to freedom of expression and opinion amounts to a violation and "any form of effort to coerce the holding or not holding of any opinion" is prohibited under the ICCPR.[37]

ii. Potential limitations on right to freedom of expression and opinion

While the right to freedom of expression must be protected, it, like other fundamental freedoms, is not an absolute right and may be subjected to narrowly tailored exceptions in limited situations. Article 19(3) of the ICCPR provides that the right to freedom of expression and opinion can be "subject to certain restrictions" but that these restrictions must be provided by law and necessary for a legitimate purpose such as (i) ensuring respect of the rights or reputations of others, or (ii) protecting national security, public order or public health or morals.

Provided by law

Article 19(3) expresses the general principle of legality, which mandates that any restriction on a right be provided by law. The UN Human Rights Committee has provided guidance that laws imposing restrictions on the rights to free expression and opinion must be promulgated with enough precision to enable individuals to adjust their conduct accordingly, and provide relevant guidance to those charged with executing the laws to ensure they can clearly ascertain which kinds of expression fall under restrictions and which do not. Such laws should not allow for "unfettered discretion for the restriction of freedom of expression on persons charged with its execution", and the laws must not otherwise contravene international human rights law or standards.[38]

35 CCPR/C/GC/34, para 7.
36 CCPR/C/GC/34, para 8.
37 CCPR/C/GC/34, paras 9, 10.
38 CCPR/C/GC/34, paras 25, 26.

Necessity and proportionality

Any restriction must be for a legitimate purpose, and, in the express terms of article 19(3), must be necessary, and the least restrictive means, to achieve that purpose. The principles of necessity and proportionality must therefore guide the restriction or limitation on the right to free expression or opinion, even where a legitimate purpose has been identified for such limitation. The UN Human Rights Committee clarifies that the test of necessity entails that limitations cannot be imposed where protection can be provided through other measures that do not restrict fundamental freedoms, while the test of proportionality guides that limitations should be proportionate to their function, not be overboard and be the "least intrusive instrument amongst others to achieve their protective function".[39]

States seeking to impose such limitations must "demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat".[40] Restrictions must "not put in jeopardy the right itself" and be implemented narrowly for the legitimate purposes provided for under article 19.[41]

With respect to the protection of the right to freedom expression where States act to place limitation based on national security objectives, the UN Human Rights Committee has explained that "extreme care must be taken" by States to ensure that "treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise are crafted and applied in a manner that conforms to the strict requirements" of article 19(3) of the ICCPR.[42] It has also given guidance that "in circumstances of public debate concerning public figures in the political domain and public institutions, the value placed by the Covenant upon uninhibited expression is particularly high".[43] Similarly, the UN Human Rights Council in its Resolution 12/16 has stressed that States should refrain from limiting "discussion of government policies and political debate; reporting on human rights, government activities and corruption in government; engaging in election campaigns, peaceful demonstrations

39 CCPR/C/GC/34, paras 33 to 35.
40 CCPR/C/GC/34, para 35.
41 CCPR/C/GC/34, paras 21, 22.
42 CCPR/C/GC/34, para 30.
43 CCPR/C/GC/34, para 38.

or political activities, including for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups".[44]

iii. Obligations to protect that may restrict expression and opinion

Article 20 of the ICCPR provides for two situations where States are not only permitted to restrict the right to freedom of expression and opinion, but are obligated to do so. Article 20 specifically provides that:

"1. Any propaganda for war shall be prohibited by law.

2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."

The UN Human Rights Committee has made clear that articles 19 and 20 of the ICCPR are "compatible with and complement each other" and that the acts prohibited under article 20 are restricted pursuant to article 19(3), and must be justified "in strict conformity" with article 19.[45] In other words, the implementation of legal prohibitions detailed under article 20 must comply with the principles of legality, legitimacy, necessity and proportionality.

Article 4 of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) similarly prohibits expression which incites

"racial hatred or discrimination" – or "hate speech". In the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence ('Rabat Plan of Action') launched in 2013, it was clearly established that in balancing the right to free expression and opinion and the prohibition of hate speech, measures taken by States must also comply strictly with article 19(3).[46]

44 This was highlighted in Communication No. IND 15/2015 from UN Special Rapporteurs on freedom of expression, cultural rights and on the situation of human rights defenders to the Government of India, relating in relation to article 124A of India's Penal Code which criminalizes sedition, 10 December 2015, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=15983

45 CCPR/C/GC/34, paras 50, 52.

46 Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, Available at: https://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

In a report released in October 2019 focusing on regulation of hate speech online, the UN Special Rapporteur on freedom of expression reasserted the applicability of articles 19 and 20 of the ICCPR, article 4 of the ICERD and the Rabat Plan of Action to the online sphere, emphasizing that existing or emerging domestic laws to prevent online hate speech must be guided by these instruments, be subject to the "requirements of legality, necessity and proportionality, and legitimacy" and to "robust public participation".[47]

iv. The right to effective remedy

The right to an effective remedy for human rights violations is a general principle of law. States are obliged to provide equal and effective access to justice to victims of rights violations, and to ensure victims are provided effective remedy and reparation.[48] Article 8 of the UDHR expresses the principle of the right to effective remedy, while article 2(3) of the ICCPR provides that effective remedy should be granted "notwithstanding that the violation has been committed by persons acting in an official capacity" and that the State should ensure "competent authorities shall enforce such remedies when granted".[49]

The right to remedy includes the State obligation to "take appropriate legislative and administrative and other appropriate measures to prevent violations" and "investigate violations effectively, promptly, thoroughly and impartially".[50] States must take measures to ensure remedies should be accessible, prompt, effective and available before an independent authority.[51]

47 Report of the Special Rapporteur on the promotion and protection of the freedom of opinion and expression, A/74/486, 9 October 2019 ('A/74/486'), para 57(b).
48 Principle 3 of the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law.
49 The right to remedy is also enshrined under article 6 of the CERD, article 39 of the CRC and article 14 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT).
50 Principle 3 of the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law.
51 See ICJ, 'The Right to a Remedy and Reparation for Gross Human Rights Violations: A Practitioners' Guide, Revised Edition 2018', Available at: https://www.icj.org/the-right-to-a-remedy-and-reparation-for-gross-human-rights-violations-2018-update-to-practitioners-guide-no-2/

v. Protection of rights to freedom of expression, opinion and information online

The obligation to ensure the protection of human rights law applies not only within a country, but may also apply extraterritorially, and at the very least to all persons within a State's jurisdiction. International human rights law is therefore generally applicable to cyberspace, because of the ubiquity of cyberspace and the numerous points of jurisdictional contact States will inevitably have across that space. The UN High Commissioner of Human Rights outlined this scope in his 2014 report on the right to privacy in the digital age.[52]

The international legal standards governing the online sphere has been the subject of ongoing commentary and guidelines promulgated at the international level to ensure protection of the rights to free expression, opinion and information online. Both treaty and non- treaty-based standards have reaffirmed that international law and standards apply both on and offline.

In July 2018, the UN Human Rights Council adopted by consensus a resolution ('UN HRC 2018 resolution') affirming that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".[53] In November 2016, the African Commission on Humans and Peoples Rights (ACHPR) adopted similar language in its resolution on the Right to Freedom of Information and Expression on the Internet in Africa affirming that human rights principles apply equally online as they do offline.[54] This was in line with an unequivocal clarification by the UN Special Rapporteur on freedom of expression in 2011 that:

52 Report of the Office of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', A/HRC/27/37, 30 June 2014 ('A/HRC/27/37'), paras 31 to 36.

53 UN Human Rights Council, 'The promotion, protection and enjoyment of human rights on the Internet', 4 July 2018, UN Doc No. A/HRC/38/L.10/Rev.1 ('A/HRC/38/L.10/Rev.1'), p3; This reiterated the same principle expressed in an earlier 2016 resolution, which had also been adopted by consensus by the UN Human Rights Council.

54 African Commission on Humans and People's Rights, 'Resolution on the Right to Freedom of Information and Expression on the Internet in Africa', ACHPR/Res. 362(LIX) 2016, Available at: https://africaninternetrights.org/updates/2016/12/article-734/

"By explicitly providing that everyone has the right to express him or herself through any media, the Special Rapporteur underscores that article 19 of the Universal Declaration of Human Rights and the Covenant was drafted with foresight to include and to accommodate future technological developments through which individuals can exercise their right to freedom of expression. Hence, the framework of international human rights law remains relevant today and equally applicable to new communication technologies such as the Internet."[55]

In June 2011, a Joint Declaration on Freedom of Expression and the Internet ('2011 Joint Declaration') issued by the UN Special Rapporteur on freedom of expression and three rapporteurs with regional mandates for free expression, clarified that the right to free expression applies to the internet, and that restrictions are "only acceptable if they comply with established international standards, including that they are provided for by law, and that they are necessary to protect an interest which is recognized under international law (the 'three-part' test)".[56] A 2015 Joint Declaration signed by the same four rapporteurs on Freedom of Expression and Responses to Conflict Situations ('2015 Joint Declaration') reasserted the application of the 'three-part' test[57] to the protection of free expression online and provided further guidance that "all criminal restrictions on content – including those relating to hate speech, national security, public order and terrorism/ extremism – should conform strictly to international standards, including by not providing special protection to officials and by not employing vague or unduly broad terms".[58]

55 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27, 16 May 2011, para 21.

56 United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and the Internet', 1 June 2011 ('Joint Declaration on Freedom of Expression and the Internet'), para 1a. Available at: https://www.osce.org/fom/78309?download=true

57 The right to free expression can only be limited if the limitation is (i) strictly provided by law (principle of legality); (ii) to pursue a legitimate aim (principle of legitimacy); and (iii) necessary and proportionate to achieve that aim (principle of necessity and proportionality). See Section II (ii).

58 United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 'Joint Declaration on Freedom of Expression and Responses to Conflict Situations', 27 April 2015 ('Joint Declaration on Freedom of Expression and Responses to Conflict Situations'), paras 2c, 3a. Available at: https://www.osce.org/fom/154846?download=true

Speaking particularly to hate speech online the UN Special Rapporteur on freedom of expression clarified in a report released in October 2019 that the ICCPR, ICERD and the Rabat Plan of Action apply equally online and emphasized that while "online hate is no less harmful because it is online", it can "incite grave offline harm" due to the "speed of reach of dissemination" of digital technologies.[59] His report not only emphasized the importance of State obligations to protect against incitement to violence online, but also asserted the crucial need for ICT companies to implement a human rights-based approach to its business models and ensure protections for human rights in accordance with the UN Guiding Principles on Business and Human Rights.[60]

UN Guiding Principles on Business and Human Rights

The UN Guiding Principles on Business and Human Rights ('UNGPs'), endorsed by the UN Human Rights Council in June 2011, sets out guidelines for States and business enterprises – including ICT companies – to protect against, prevent and remedy human rights violations committed in business operations.[61] These principles are grounded in a UN framework for business and human rights which rests on three pillars: the State's duty to protect against human rights violations; the corporate responsibility to respect human rights and greater access to effective remedy – judicial or non-judicial – by victims of violations.[62]

The UNGPs clarify that, even with respect to the exercise of rights on platforms regulated entirely by ICT companies, States retain a primary duty to enact appropriate and effective laws, policies and regulations to ensure protection against violations of those rights online. This duty also extends to taking necessary and appropriate measures to ensure that where violations occur, victims have access to effective remedy through judicial mechanisms or other administrative, legislative or regulatory means. While

59 UN News, 'Companies 'failing' to address offline harm incited by online hate: UN expert', 21 October 2019, Available at: https://news.un.org/en/story/2019/10/1049671; A/74/48050, paras 4 to 18.

60 A/74/486, para 42; The UN Special Rapporteur's report presented clear recommendations for ICT companies to integrate international human rights law and standards into their operations and practices. This paper acknowledges that the conduct of ICT companies is a crucial factor with respect to protection of the rights to expression, information and privacy online. For the purposes of this paper, however, the focus will be limited to in-depth analysis of the obligations of States to protect these rights.

61 These principles built on a framework for business and human rights proposed by the Special Representative to Secretary-General, John Ruggie, and approved by the UN Human Rights Council in 2008.

62 UN Guiding Principles on Business and Human Rights, HR/PUB/11/04, 2011, Available at: https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf

ICT companies have obligations to ensure human rights are protected in the course of their operations and provide effective remedy where rights violations occur, States are obliged to exercise an overarching oversight and regulatory role to ensure that corporations comply with these obligations.

Tshwane Principles

With respect to the right to information, the Global Principles on National Security and the Right to Information ('Tshwane Principles') were adopted by in October 2013 in a process involving some 500 intergovernmental and independent experts and civil society and academic groups, including the ICJ.[63] These Principles give detailed guidance on protecting the right to information and ensuring public access to information held by States, in a way that does not jeopardize legitimate efforts to ensure protection of individuals from security threats.[64] These principles, which were drafted to respond to increased use of digital technologies for information dissemination and a rise in the development of right to information laws, set out protections for whistleblowers, limitations on secrecy with respect to information held by States, and the parameters of the right to information of the public.[65]

Key guidelines in the Tshwane Principles provide, *inter alia*, that every individual has a right of access to information held by public authorities, including "business enterprises within the national security sector, including private military and security companies", "subject only to limited exceptions prescribed by law and necessary to prevent specific, identifiable harm to legitimate interests, including national security" (Principle 1); that States must always disclose information pertaining to "gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security" (Principle 10A); that States

63 ICJ, 'Council of Europe endorses global principles on the right to information', 2 October 2013, Available at: https://www.icj.org/council-of-europe-endorses-global-principles-on-the-right-to-information/

64 The development of these Principles followed more than two years of consultations with more than 500 experts from more than 70 countries from the government, security and civil society sectors. The process also involved working closely with the four special rapporteurs on freedom of expression and the media from the UN, the African Commission on Human and Peoples' Rights, the Organization of American States (OAS), and the Organization for Security and Cooperation in Europe (OSCE), as well as with the UN Special Rapporteur on Counter-Terrorism and Human Rights. See ICJ, 'New global principles on the right to information launched', 12 June 2013, Available at: https://www.icj.org/new-global-principles-on-the-right-to-information-launched/; Justice Initiative, 'Global Principles on National Security and the Right to Information', Available at: https://www.justiceinitiative.org/uploads/45d4db46-e2c4-4419-932b-6b9aadad7c38/tshwane-principles-15-points-09182013.pdf

65 *Ibid.*

should not keep secret "information… material" to victims' claims for remedy or reparation (Principle 30); that individuals who are not public servants, including journalists, should not be prosecuted for receiving, possessing or disclosing classified information to the public (Principle 47); and that States should only withhold information on national security grounds "for only as long as necessary to protect a legitimate national security interest" and that such withholding must be "reviewed periodically" (Principle 16).[66]

These expand on the earlier Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Freedom of Expression and Access to Information, adopted in October 1995. They also reinforced the rights to freedom of expression, opinion and information and provided guidelines to protect the "right to obtain information from public authorities, including information relating to national security", providing that no limitations on this right are permitted "unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest".[67]

vi. The right to privacy

The right to privacy is recognized by the UN General Assembly as "one of the foundations of a democratic society", and a pre-requisite to the free and independent exercise of the rights to expression and to hold opinions without interference.[68] Article 12 of the UDHR and article 17 of the ICCPR accordingly protect the right of every individual against arbitrary or unlawful interference with his or her privacy.[69] While not set out expressly in article 17, the Human Rights Committee and the Human Rights Council have both affirmed that the principles of legality, necessity, and proportionality, apply to the right to privacy in the same manner as they do to freedom of expression and other fundamental freedoms.

66 Global Principles on National Security and the Right to Information, 2013, Available at: https://www.icj.org/wp-content/uploads/2013/06/Global-Principles-on-National-Security-and-the-Right-to-Information-Tshwane-Principles-June-2013.pdf

67 The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, Available at: https://www.article19.org/wp-content/uploads/2018/02/joburg-principles.pdf

68 UN General Assembly, 'The right to privacy in the digital age', A/RES/68/167 ('A/RES/68/167'), 18 December 2013, Available at: https://undocs.org/A/RES/68/167

69 Article 17 of the ICCPR reads "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks".

Challenges in protecting the right to privacy have dramatically increased in the digital era, as "the Internet has become both ubiquitous and increasingly intimate".[70] In December 2013, the UN General Assembly adopted resolution 68/167 which noted that accelerated developments in ICT had expanded the capacity of States, private corporations, and other non-State actors to collate, surveil and intercept data in a manner that infringes upon the right to privacy and other rights, and affirmed that States were obliged under international human rights law to prevent violations committed in the context of digital communications.[71]

International legal principles apply equally to privacy online as offline. In September 2013, the Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance ('Necessary and Proportionate Principles') was launched at the UN Human Rights Council, which reaffirmed that international legal principles of legality, legitimacy, necessity and proportionality were equally relevant and enforceable within the context of the digital environment, particularly with respect to communications surveillance technologies and techniques.[72] These principles, developed through broad consultations between privacy, security, human rights and digital rights experts across the world, were adopted by more than 400 organizations globally. A final version was adopted in May 2014.

Standards governing the right to privacy online continue to evolve. In 2015, the UN Human Rights Council appointed the first UN Special Rapporteur on the right to privacy within the digital context, who in 2018, reported to the Council that while progress had been made with respect to international standards on surveillance, further development was required.[73] At the same time, the Special Rapporteur observed that more efforts were required to "explore the intersection of privacy and security and State behaviour in cyberspace … in a determined attempt to develop a more comprehensive legal framework for the Internet".[74]

70 A/HRC/27/37, para 1.
71 A/RES/68/167.
72 Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance, May 2014, Available at: https://necessaryandproportionate.org/principles; The ICJ is also a signatory to these Principles. In his 2014 report following on from resolution 68/167, the UN Office of the High Commissioner for Human Rights referred to the Necessary and Proportionate Principles, reiterating that the "overarching principles of legality, necessity and proportionality" apply to limitations on the right to privacy online. See A/HRC/27/37, para 23.
73 Report of the UN Special Rapporteur on the right to privacy, A/HRC/37/62, 25 October 2018 ('A/HRC/37/62'), Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/324/47/PDF/G1832447.pdf?OpenElement
74 A/HRC/37/62, paras 129 to 131.

EU GDPR and Convention 108+

At the regional level, the European Union (EU) has made efforts towards developing concrete legal guidelines with respect to protection of online personal data. In May 2018, the EU General Data Protection Regulation (GDPR) came into force, providing protections for privacy and data breaches with penalties of up to 4 percent of an organization's annual global turnover or €20 million (approx. US$22 mil.) for severe infringements.[75] Crucially, the GDPR applies extraterritorially to any company processing the data of subjects within the EU, regardless of the location of the company.[76] Following the coming into force of the GDPR, in January 2019, Google was fined €50 million (approx. US$55 mil.) by French data protection regulator, CNIL, for failing to obtain consent from its users to use their personal data for targeted advertising.[77] In March 2019, the EU also set out a latest draft of its 'ePrivacy Regulation', focusing on privacy protections for data processed on electronic communication services.[78]

While the impacts of these newer, consolidated European data protection laws remain to be seen, their implementation will provide precedential guidance for global efforts to develop laws to protect the right to privacy in the online sphere.[79] A key example is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal

75 Information on the GDPR is available at: https://eugdpr.org/the-regulation/; In May 2018, the EU Data Protection Law Enforcement Directive also came into force, protecting the right of EU citizens to data protection where personal data is processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. The Directive is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

76 GDPR, Article 3, Available at: https://gdpr-info.eu/art-3-gdpr/; One commentary noted that this was "part of a global trend to extend the scope of data protection laws to make them reflect the borderless nature of the Internet", See Adele Azzi, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation' (2018) 9 JIPITEC 126, Available at: https://www.jipitec.eu/issues/jipitec-9-2-2018/4723

77 Klint Finley, 'EU Privacy Law Snares Its First Tech Giant: Google', *WIRED*, 22 January 2019, Available at: https://www.wired.com/story/eu-privacy-law-snares-first-tech-giant-google/; Chris Fox, 'Google hit with £44m GDPR fine over ads', *BBC,* 21 January 2019, Available at: https://www.bbc.com/news/technology-46944696; This was not the first fine to be issued under the GDPR, See Jon Porter, 'Google fined €50 million for GDPR violation in France', *The Verge,* 21 January 2019, Available at: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

78 Regulation of the European Parliament and the Council concerning the respect for private life and protection of personal data in electronic communications repealing Directive 2002/58/EC. This draft is available at: https://data.consilium.europa.eu/doc/document/ST-7099-2019-INIT/en/pdf

79 In his 2018 report to the UN General Assembly, the Special Rapporteur on the right to privacy noted, "It is likely, in the next five to ten years, that the extraterritorial effects of GDPR with the ever-widening club of Convention 108 countries, will have a significant effect on the deepening world-wide privacy culture. The precise nature of this evolution is still emerging, as is its relevance to the need for further developments such as stand-alone principles for Big Data and Open Data." See Report of the UN Special Rapporteur on the right to privacy [Advanced Unedited Version], A/73/45712, 17 October 2018 ('A/73/45712'), para 101.

Data (Convention 108) – the most comprehensive existing international instrument on personal data protection which is open to accession by any State.[80] The modernization of Convention 108 (now 'Convention 108+') in May 2018 included many elements of the GDPR, and its revision was a welcome effort to combat new challenges presented by developing ICTs.[81] However, time is required to assess the impacts of implementation of both the GDPR and Convention 108+.[82]

vii. Extraterritoriality

A fundamental challenge that has arisen in respect of human rights protection in the online sphere is a jurisdictional one. While enforcement of human rights obligations has traditionally been given effect through the apparatus of States, cyberspace operates across and beyond such territorial boundaries.

International human rights law, however, similarly applies across and beyond boundaries in obliging human rights to be protected not only within a State territory but also in territories where States exercise effective control or any place where it may otherwise have jurisdiction.[83] The 2014 OHCHR report on privacy online clarified that, within the online sphere, extraterritorial obligations of States pursuant to article 2 of the ICCPR and the principle of non-discrimination apply to violations committed in cyberspace.[84] International human rights law has also been clarified to apply to non-State actors such as technological companies.[85] The question therefore does not concern the applicability of international human rights standards *per se* to

80 Convention 108 was promulgated by the Council of Europe in 1981, but is open to accession by any State. As of October 2018, including 47 European States, Uruguay, Mauritius, Senegal, Tunisia, Morocco, Cape Verde, Argentina, Mexico, and Burkina have requested accession to the Convention. Eleven other countries, or their data protection authorities, are Observers on its Consultative Committee. See A/73/45712, footnote 83.

81 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018), Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

82 A/73/45712, para 101.

83 This was affirmed by the Maastricht Principles on Extraterritorial Obligations of States, which clearly defined the scope and nature of State obligations to individually and jointly respect, protect and fulfil economic, social and cultural rights defined beyond their borders. These principles are available at: https://www.fidh.org/IMG/pdf/maastricht-eto-principles-uk_web.pdf; The existence of State obligations 'diagonally' to persons in other countries is clarified in articles of the UN Charter, UDHR, ICCPR and ICESCR, as noted by Sarah Joseph, 'Blame it on the WTO?: A Human Rights Critique', 2011, under 'Extraterritorial Human Rights Duties', Available at: https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199565894.001.0001/acprof-9780199565894-chapter-9

84 A/HRC/27/37, paras 31 to 36.

85 Corporate responsibility to respect and protect human rights was affirmed by the UN Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework, Endorsed by UN Human Rights Council Resolution 17/4 of 16 June 2011, Available at: https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf

cyberspace, but the manner in which effective enforcement can be ensured.

In a lecture delivered in September 2017, Professor Yuval Shany, now Chair of the UN Human Rights Committee, wondered if a specialized framework needed to be developed for the internet – *lex cybernetica* – guided by 'traditional' international human rights law. As he keenly observed:

"The chief attribute that makes cyberspace such a useful and powerful vehicle for communication and access to data and ideas … is its universality: It is a space shared by all and freely accessible to all under more or less equal terms pursuant to the net neutrality principle. An IHRL framework that requires states to renationalize segments of cyberspace and to fragment it to overlapping territorial zones of influence and regulation, cuts against the logic of creating such a space, and may result in 'throwing the baby with the bath water'".[86]

While the effectiveness of international legal enforcement mechanisms, such as the GDPR and Convention 108+, remains to be assessed there is no doubt that extraterritorial obligations to protect human rights extend to States and non-State actors equally online as offline under international human rights law.

viii. The rights to peaceful assembly, freedom of association, and political participation

The rights to freedom of association, assembly, and political participation are also engaged when individuals engage in online communications and information-sharing. These rights are protected respectively under articles 21, 22 and 25 of the ICCPR. The ICCPR provides for no restrictions to be placed on these rights unless necessary and proportionate for a legitimate aim:

"Article 21 – The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others.

86 Prof. Yuval Shany, 'Cyberspace: The Final Frontier of Extra-Territoriality in Human Rights Law', 26 September 2017, Available at: https://csrcl.huji.ac.il/people/cyberspace-final-frontier-extra-territoriality-human-rights-law

Article 22 – 1. Everyone shall have the right to freedom of association with others …

2. No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on members of the armed forces and of the police in their exercise of this right.

Article 25 – Every citizen shall have the right and the opportunity, without … unreasonable restrictions:

(a) To take part in the conduct of public affairs, directly or through freely chosen representatives."

While this paper focuses mainly on the rights to free expression, opinion, information and privacy, it should be stressed that these rights often concurrently engage the rights to peaceful assembly, freedom of association and political participation. These linkages are made explicit in the draft General Comment No. 37 on the right to peaceful assembly under article 21, currently under discussion by the Human Rights Committee. It notes that in the digital era, exercise of the right to peaceful assembly often occurs online or depends on the use of digital services, and that these activities too are protected under article 21.[87]

The current draft establishes that State control of access to the internet, such as restrictions on connectivity, can infringe on the rights to free expression, association and assembly. Any such restriction should be in line with the 'three-part' test for limiting freedom of expression and information:

"States parties should … refrain from unduly blocking Internet connectivity in relation to demonstrations. The same applies to geo-targeted or technology-specific interference or hindering of connectivity. States should ensure that self-regulation by Internet service providers does not unduly affect assemblies and that the activities of those providers does not unduly infringe upon the privacy of assembly participants. Any restriction on the

87 Draft of UN Human Rights Committee, General Comment No. 37 on Article 21: the right to peaceful assembly ('Draft GC No. 37'), para 38, Available at: https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx; The HR Committee commenced its first reading of the draft during its 126th session in July 2019.

operation of information dissemination systems must conform with the test for restrictions on freedom of expression. At the same time, the fact that people can communicate online should not be used as a ground for undue restrictions on in-person assemblies."[88]

It thereafter clarifies how the rights to assembly and association intertwine with others protected under the ICCPR in the context of surveillance or data monitoring:

"The mere fact that participants in assemblies are out in public does not mean that their privacy cannot be infringed, for example, by facial recognition and other technologies that can identify individual participants in mass assemblies. The same applies to the monitoring of social media. Independent scrutiny and oversight must be exercised over the collection of personal information and data of those engaged in peaceful assemblies. … The surveillance of those involved in assemblies and other data-gathering may violate their privacy (art. 17). Freedom of assembly is more than a manifestation of freedom of expression (art. 19 (2)), but it has an expressive element and the rationale for the recognition of these two rights and the acceptable limitations overlap in many ways. Freedom of information (art. 19 (2)) underlies the ability of participants to know about the legal and administrative framework within which they participate in assemblies and enables the public to hold government officials accountable. Freedom of association (art. 22) also protects collective action, and restrictions on this right often affect freedom of assembly. Like freedom of expression, the right of political participation (art. 25) is closely linked to peaceful assembly. The right to non-discrimination protects participants against discriminatory practices in the context of assemblies (art. 26)."[89]

Human rights defenders

Human rights defenders use online platforms to exercise and to promote the rights to association, assembly and political participation, and other rights. Many human rights defenders face harassment, intimidation, threats to personal security and other attacks by State or non-State actors, which now extend to the online sphere. Human rights defenders face more contemporary threats such as infringements of their digital security, privacy and dignity from online attacks and smear campaigns, which often also

88 Draft GC No. 37, para 38.
89 Draft GC No. 37, paras 72, 112.

worsen pressure, intimidation and security risks they face offline. In a report released in 2019, the UN Special Rapporteur on the situation of human rights defenders highlighted increased harassment, incitement to violence and attacks online against women human rights defenders in particular, including shaming, attacks on honour, threats of sexual violence, verbal abuse and doxxing – where private information about a person is disseminated online without her consent.[90] In December 2018, the UN Special Rapporteur and four rapporteurs with regional mandates on human rights defenders also recognized increased threats faced by human rights defenders online.[91]

The UN Declaration on Human Rights Defenders provides that States must act to protect and support human rights defenders in their work, through adopting necessary legislative, administrative or other measures to ensure protection of their rights to association, assembly and political participation, among others, not only offline but also online.[92]

ix. International standards and commentary pertaining to internet restrictions and shutdowns

Internet shutdowns – banning access to the internet in general or restricting access to specific online platforms – have emerged as a blunt tool used by governments around the world to protect national security and public order at the risk of violating a wide range of rights.[93] Today, individuals rely on the internet not only to communicate with others, but also for a vast array of services and transactions, all of which are impacted

90 Report of the UN Special Rapporteur on the situation of human rights defenders, A/HRC/40/60, 10 January 2019, Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/004/97/PDF/G1900497.pdf?OpenElement

91 United Nations (UN) Special Rapporteur on the Situation of Human Rights Defenders, Special Rapporteur of the African Commission on Human and People's Rights (ACHPR) on Human Rights Defenders, Council of Europe Commissioner for Human Rights, First Deputy Director of OSCE Office for Democratic Institutions and Human Rights (ODIHR), Rapporteur on Human Rights Defenders of the Inter-American Commission for Human Rights (IACHR), 'Joint Statement: 20 years on from the adoption of the UN Declaration on Defenders: The protection of human rights defenders is non-negotiable', 18 December 2018, Available at: https://www.coe.int/en/web/commissioner/-/20-years-on-from-the-adoption-of-the-un-declaration-on-defenders-the-protection-of-human-rights-defenders-is-non-negotiable

92 Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, A/RES/53/144, December 1998, Available at: https://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration.pdf

93 In 2016, RightsCon Brussels, which brought together stakeholders from the policy, human rights and ICT sectors, defined an internet shutdown as "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information… (which) include blocks of social media platforms, and are also referred to as "blackouts," "kill switches," or "network disruptions"." See Access Now, 'The State of Internet Shutdowns around the World: The 2018 #Keepiton Report' ('Access Now 2018 report'), p2, Available at: https://www.accessnow.org/cms/assets/uploads/2019/06/KIO-Report-final.pdf

in an internet shutdown. This infringes upon not only the rights to free expression and information, but also the rights of assembly, association, education, health, work, livelihood and security.[94] Internet shutdowns "stunt the democratic process", "batter whole economies and individual businesses", and "drastically disrupt the daily life of ordinary citizens, turning the search for mobile service into a game of cat and mouse with the police and driving people across borders just to send emails for work".[95] Internet shutdowns can also have the effect of concealing human rights violations, especially when they are imposed in areas of violence and conflict.[96]

Comprehensive internet shutdowns almost never comply with international human rights law. The UN HRC resolution adopted in 2018 "unequivocally condemned measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law" and urged all States "to refrain from and cease such measures".[97] In the 2011 Joint Declaration, the rapporteurs for freedom of expression clarified that States have a positive obligation to ensure universal access to the internet of individuals, which is derived from their obligation to promote and protect the right to freedom of expression.[98] They recognized that internet access was crucial for the promotion and protection of other rights, including the rights to assembly, association, free elections, education, health and work, and that denial of an individual's access to the internet was "a punishment (of) extreme measure, which could be justified only where less restrictive measures are not available and where ordered by a court, taking into account the impact of this measure on the enjoyment of human rights".[99]

94 "Internet shutdowns curtail freedom of expression, cut access to information, and can inhibit people from assembling and associating peacefully, online and off. In addition, during shutdowns, many victims are unable to reach their families, get accurate information to stay safe, or reach emergency services. Shutdowns disrupt businesses, schools, and ordinary lives, often exacting a significant financial cost." Access Now 2018 report, p2.

95 Patrick Kingsley, 'Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards', *New York Times,* 2 September 2019 ('NY Times, 2 September 2019'), Available at: https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html?te=1&nl=morning-briefing&emc=edit_MBAE_p_20190902&section=longRead?campaign_id=7&instance_id=120678segment_id=16669&user_id=3f72f2845ba8594bb0e4459957511f9b&regi_id=87913927ion=longRead

96 Access Now 2018 report, pp 13, 14.

97 A/HRC/38/L.10/Rev.1, p5.

98 Joint Declaration on Freedom of Expression and the Internet, paras 6a, 6e.

99 Joint Declaration on Freedom of Expression and the Internet, paras 6a, 6c. For example, news reports have detailed how an ongoing shutdown in Kashmir has disrupted crucial communications between doctors, patients, healthcare providers and patients, resulting in preventable deaths, drug shortages and a reduced number of surgeries, with pediatric care and maternity services "among the hardest hit". See Sameer Yasir, Jeffrey Gettleman, 'In Kashmir, a Race Against Death, With No Way to Call a Doctor', *New York Times,* 7 October 2019, Available at: https://www.nytimes.com/2019/10/07/world/asia/kashmir-doctors-phone.html?te=1&nl=morning-briefing&emc=edit_MBAE_p_20191007&section=longRead?campaign_id=7&instance_id=12908&segment_

The Joint Declaration further emphasized that "cutting off access to the internet, or parts of the internet, for entire populations or segments of the public … can never be justified, including on public order or national security grounds".[100] In the 2015 Joint Declaration, they re-emphasized that "using communications 'kill switches' (i.e. shutting down entire parts of communications systems)… are measures which can never be justified under human rights law".[101] Internet shutdowns have also been condemned as violations of international human rights law by the FOC in its 2017 Joint Statement on State Sponsored Network Disruptions.[102]

x. Other efforts to develop international normative standards governing cyberspace

While preceding sections of this report have looked at treaty and non-treaty based guidance on applying international legal standards to the online sphere, this section considers other multi-lateral initiatives led by States, policy "think-tanks", international organizations and private ICT sector companies which have proposed international standards to govern cyberspace – including standards to ensure cybersecurity, through protections for information security online and against cyber-attacks.

Such multi-lateral efforts have lacked adequate grounding in international human rights law and standards and are limited as they do not have the status of international instruments. These include the Shanghai Cooperation Organization's (SCO) International Code of Conduct on Information Security, the Paris Call for Trust and Security in Cyberspace, the Global Commission on the Stability of Cyberspace, the Global Forum on Cyber Expertise and the Freedom Online Coalition's (FOC) Working Group on 'An Internet Free and Secure'.[103] The SCO International Code of Conduct on

id=17671&user_id=3f72f2845ba8594bb0e4459957511f9b&regi_id=87913927ion=longRead; Human Rights Watch, 'Kashmir Shutdown Raises Healthcare Concerns', 30 August 2019, Available at: https://www.hrw.org/news/2019/08/30/kashmir-shutdown-raises-healthcare-concerns

100 Joint Declaration on Freedom of Expression and the Internet, para 6b, also clarifying that "The same applies to slow-downs imposed on the Internet or parts of the Internet".

101 Joint Declaration on Freedom of Expression and Responses to Conflict Situations, para 4c.

102 Freedom Online Coalition, 'Joint Statement on State Sponsored Network Disruptions', March 2017, Available at: https://www.freedomonlinecoalition.com/wp-content/uploads/2017/03/FOC-Joint-Statement-on-State-Sponsored-Network-Disruptions.pdf

103 France Diplomatie, 'Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace', November 2018, Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in; Global Commission on the Stability of Cyberspace, 'Global Commission Introduces Six Critical Norms Towards Cyber Stability', 8 November 2018, Available at: https://cyberstability.org/news/global-commission-introduces-six-critical-norms-towards-cyber-stability/; See updated draft of SCO International code of conduct for information security submitted in January 2015 to the UN Secretary-General, 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation,

Information Security, which was presented to the United Nations' Secretary-General by Member States of the SCO in 2011 and then in 2015 in updated form, did not refer to the right to privacy at all and focuses on national security and preserving State "sovereignty".[104]

The FOC's 'Recommendations for Freedom Online' (also known as the 'Tallinn Agenda') affirms that the "same rights that people have offline must also be protected online" and signals the commitment of its 30 Member States to "adopt and encourage policies and practices, nationally and internationally, that promote the protection of human rights. " However, it fails to draw clear links between international legal standards –including the obligations on States – and the realization of these commitments.[105] Proposals developed by private ICT sector companies, including for example, Microsoft, Siemens, Nornickel and Google, and by academic coalitions or think-tanks, such as the Global Commission on the Stability of Cyberspace and the Bright Internet Agenda, proposing norms governing information security and protection against cyber-attacks face similar limitations.[106]

International efforts to negotiate normative standards governing cybersecurity have been fragmented and inconsistent. A fundamental challenge is the difference of interpretation between States about the application of international human rights and humanitarian law to cybersecurity and cyber conflicts.[107] At the UN level, two separate mechanisms currently exist, working in parallel on the regulation of cyberspace within the context of international security, led by States with different visions – the United States and the Russian Federation.[108]

Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General', 13 January 2015, UN Doc. A/69/723, Available at: https://regmedia.co.uk/2015/02/04/un-internet-security-13jan15.pdf; Freedom Online Coalition, 'An Internet Free and Secure', Available at: https://freeandsecure.online/about/; Global Forum on Cyber Expertise, 'About the GFCE', Available at: https://www.thegfce.com/about

104 Sarah McKune, 'An Analysis of the International Code of Conduct for Information Security', *The Citizen Lab*, 28 September 2015, Available at: https://citizenlab.ca/2015/09/international-code-of-conduct/

105 FOC, 'Recommendations for Freedom Online', 28 April 2014, Available at: https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

106 Eneken Tikk and Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy', *Cyber Policy Institute,* 2017 ('Tikk and Kerttunen, 2017'), p5, Available at: https://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf

107 Tikk and Kerttunen, 2017, pp. 10, 11, 16, 17; Deborah Brown, 'UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online', Association for Progressive Communications, 10 January 2019 ('APC, 10 January 2019'), Available at: https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed

108 Disagreement in the UN General Assembly's First Committee focusing on disarmament and international security in the cyber sphere led to the United States and Russia putting forth two separate resolutions – the US-led resolution mandated the creation of a new GGE to continue the GGE process "to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the

For these reasons, international human rights standards are essential to inform solutions and bridge interpretive and political differences. In 2013 and 2015, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) produced two reports which set out recommendations to improve ICT security on a global level. The GGE's 2013 report included one recommendation that State efforts to ensure cybersecurity must "go hand-in-hand with respect for human rights and fundamental freedoms set forth in international instruments". Its 2015 report went further to call on States to "respect" UN resolutions protecting human rights on the internet and the right to privacy online.[109] The GGE's recommendations, however, did not provide targeted guidelines for implementing human rights protections, such as those pertaining to free expression, information and privacy. In September 2019, 27 nations signed a 'Joint Statement on Advancing Responsible State Behaviour in Cyberspace' affirming their "commitment to uphold the international rules-based order and encourage its adherence, implementation, and further development, including at the ongoing UN negotiations".[110]

sphere of information security", while the Russia-led resolution mandated the setting up of an Open-Ended Working Group (OEWG) "acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation". See APC, 10 January 2019; UNGA Resolution No. 73/27, 'Developments in the field of information and telecommunications in the context of international security', 5 December 2018, UN Doc. No. A/RES/73/27 ('A/RES/73/27'); UNGA Resolution No. 73/266, 'Advancing responsible State behaviour in cyberspace in the context of international security', 22 December 2018, UN Doc. No. A/RES/73/266 ('A/RES/73/266').

109 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', 24 June 2013, UN Doc. No. A/68/98, para 21; The GCE's 2015 report referred specifically to Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, and General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age. See Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security', 22 July 2015, UN Doc. No. A/70/174, para 13(e).

110 These 27 nations were Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Spain, Sweden, the United Kingdom, and the United States. The statement noted that they would abide by the international rules-based order at both the ongoing UN negotiations of the Open Ended Working Group and Group of Governmental Experts. See fn 98 on the OEWG. US Department of State, 'Joint Statement on Advancing Responsible State Behavior in Cyberspace', 23 September 2019, Available at: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

III. Employing legal frameworks which serve to abusively restrict freedom of expression, opinion and information online

In Southeast Asia, legal frameworks have been systematically used and abused to control and restrict freedom of expression, opinion and information online. In some cases, existing laws which protect against defamation, sedition or national security have been used to prosecute or inappropriately regulate expression online just as they had been used to target offline expression in the past. More recently, such laws have been augmented or superseded by a new generation of laws and regulations governing telecommunications, cybersecurity and computer crimes that are tailored to target online expression and information. In both cases, criminal and administrative actions are often justified as necessary to protect individual dignity or national security, and draw a link between the spread of a "falsehood" online and its threat to such dignity or security, social stability and/or public order. These laws often conflate national or public security with the "security" of the ruling political regime or other powerful interests – who often draft, promulgate and execute, or influence the laws in the first place.

Despite the justifications offered for enforcing these laws, they have, by and large, been misapplied and arbitrarily enforced to curtail a wide range of comment on matters of public interest, including expression of critical dissent. Defamation laws, which can serve a legitimate purpose to protect the rights and reputation of persons, have been used to clamp down on free expression and opinion in *Myanmar, Thailand, Indonesia, Singapore* and *Philippines*. Problematic *lèse majesté* laws aiming to protect the reputation of the monarchy have been expanded so as to be wielded against individuals in *Thailand* and *Cambodia*. Archaic laws written to protect against sedition have been used to muzzle political expression in *Thailand, Myanmar, Malaysia, Brunei* and *Philippines* under the guise of preventing "unrest and disaffection in society". Abusive and overbroad laws advanced to protect 'national security' have been used to curtail freedom of expression and information in *Vietnam, Laos* and *Myanmar.* Contempt of court laws aiming to protect the authority of the judiciary have been misused to achieve the same effect in *Singapore, Malaysia* and *Thailand*.

More recently, legal measures to regulate information on online platforms have been used to censor expression and information online. Meanwhile, laws aiming to control the spread of disinformation online and to protect cybersecurity have been advanced, despite serious concerns that these laws will result in further suppression of online expression and information.[111]

The ICJ has identified nine areas where legal frameworks have been drafted and interpreted to unduly regulate expression and information online in ways that are not human rights compliant. By organizing the analysis in this manner, we hope to highlight commonalities across the region – both in the laws themselves as well as the arbitrary ways in which they have been implemented.

These are:

i. Laws which aim to protect the reputation of legal persons
ii. Laws which aim to protect the reputation of the monarchy
iii. Laws on sedition
iv. Laws which aim to protect the security of the nation or public order
v. Laws which aim to protect the courts

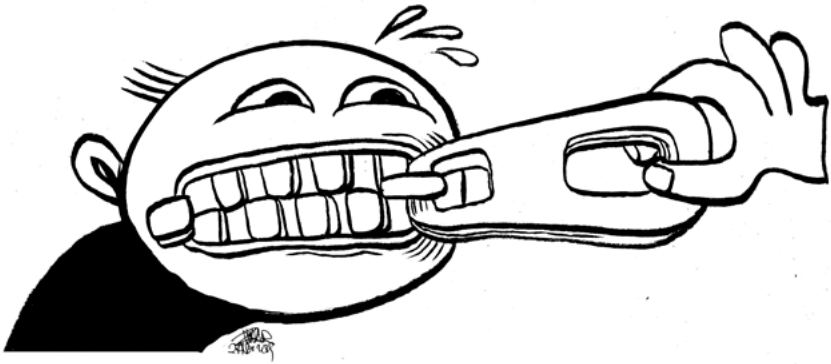
*

vi. Laws which aim to regulate information online
vii. Laws which aim to control the spread of "disinformation" online
viii. Laws which aim to protect cybersecurity
ix. Laws abused to justify internet shutdowns

111 This report is not an exhaustive representation of laws in the countries identified in this paper which have been abused to control free expression and information online. It presents only a partial reflection of deteriorating conditions in Southeast Asia. In the interests of brevity, this paper only highlights selected laws in selected countries and selected cases towards evidencing a regional trend, noting that there has been misuse of measures other than those identified in this report – including non-legal measures – to restrict freedom of expression, opinion and information online.

The first five of these areas (*Section III. a. Existing legal frameworks*) are generally part of the legal frameworks of the countries that have historically been used to clamp down on free expression and information online, even if the laws themselves were not specifically designed to address online speech. In some cases, such as sedition and lesè majesté laws in the region, centuries-old laws have been retained and misused to expand restrictions on more contemporary forms of expression online, often augmented with new legal provisions which expand government powers to regulate the internet.

The last four areas (*Section III. b. Emerging legal frameworks*) are more recent efforts aimed at controlling expression and information on the internet. These laws sometimes set up freestanding regulatory regimes affecting the internet economy, particularly social media platforms, including through the creation of new criminal causes of action or extending existing causes of action in domestic criminal legal frameworks to the online sphere. These laws pose a particular threat in that they expand States' powers to surveil and control information in the cybersphere, where vast amounts of data can be systematically retained, recovered and misused to target individuals. At the same time, there may be opportunities to engage with governments and the private sector to find human rights-sensitive ways to to address legitimate policy concerns.



(a) Existing legal frameworks

i. Laws which aim to protect the reputation of legal persons

Laws advanced to protect the reputation of legal persons against defamation – both civil and criminal – have been misused throughout the region to curtail freedom of expression and information online. This section examines how defamation provisions in *Myanmar, Thailand, Indonesia, Singapore* and the *Philippines* have been used to shield the State and other powerful actors from criticism and may impose criminal and hefty civil penalties on individuals in contravention of international human rights law and standards.

As indicated above, freedom of expression is protected under article 19 of the ICCPR. In clarifying the scope of that protection and the permissibility of State limitations on it, the UN Human Rights Committee has stressed that States that provide for criminal liability for defamation should decriminalize defamation and that "imprisonment is never an appropriate penalty" as it is neither necessary nor proportionate towards the aim of protecting the reputation of others.[112] Civil penalties, meanwhile, must not be "excessively punitive", must comply strictly with the principles of necessity and proportionality, and must be adjudicated expeditiously before an independent and impartial judicial authority in line with an individual's right to fair trial.[113]The UN Special Rapporteur on freedom of expression has similarly clarified that penalties imposed in cases of defamation should never be "so large as to exert a chilling effect on freedom of opinion and expression and the right to seek, receive and impart information", and that "penal sanctions should never be applied".[114]

The UN Human Rights Committee has further clarified that expression of opinions made with respect to public figures, including critical expressions, must be protected. Thus, authorities should refrain from sanctioning "untrue statements that have been published in error but without malice", and a public interest defence should should be available to those against whom a defamation case has been brought.[115]

112 CCPR/C/GC/34, para 47; UN Human Rights Committee, *Rafael Marques de Morais v. Angola*, Communication No. 1128/2002, CCPR/C/83/D/1128/2002 (2005), para. 3.9, Available at: https://www1.umn.edu/humanrts/undocs/1128-2002.html

113 CCPR/C/GC/34, para 47.

114 Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression, Abid Hussain, 29 January 1999, UN Doc. E/CN.4/1999/64, para. 28(h).

115 CCPR/C/GC/34, para 47.

Before looking at laws and cases from *Myanmar, Thailand, Indonesia* and *Singapore*, it is informative to consider the assessment and denunciation by the UN Human Rights Committee of the criminalization of defamation and imposition of imprisonment as punishment for defamation in the *Philippines*. While the case covered below does not involve communication of information through an online medium, it is relevant for its precedential value.

Philippines

In the Philippines, defamation is classified as a "crime against honour" under the **Revised Penal Code**, where article 353 specifically criminalizes the offence of libel and article 355 imposes a maximum penalty of imprisonment of six years for the offence.[116]

In October 2011, the UN Human Rights Committee determined that provisions under the Revised Penal Code criminalizing defamation were incompatible with Philippines' obligations under article 19 of the ICCPR. The Committee indicated that the prosecution and imposition of a prison sentence on ***Alexander Adonis***, a radio broadcast journalist, for alleged defamation, constituted a violation of his rights. Adonis had been convicted by the Regional Trial Court of Davao City under articles 353 and 355 of the Revised Penal Code, for reporting in his professional capacity on an alleged relationship between a congressman and a married television personality.[117] The court had further ordered that Adonis pay PHP 100,000 (approx. USD 1,935) as "compensation for moral damages" to the congressman and an extra PHP 100,000 as "exemplary damages" to set "an example for notorious display of irresponsible reporting".[118]

In its review of Adonis' case, the Committee also called upon the Philippine government to provide Adonis with effective remedy and adequate compensation for his imprisonment term, and called for the libel law to be reviewed to "prevent similar violations occurring in the future".[119] Committee Members Fabían Salvioli and Rajsoomer Lallah further expressed the view that the Philippines had failed to meet its obligations under article 2(2) of

116 Revised Penal Code of the Philippines, Act No. 3815 ('Revised Penal Code'), Available at: https://www.un.org/Depts/los/LEGISLATIONANDTREATIES/PDFFILES/PHL_revised_penal_code.pdf

117 The congressman filed criminal complaints against Adonis and his radio manager, following which charges against the manager were dropped.

118 UN Human Rights Committee, Communication No. 1815/2008, CCPR/C/103/D/1815/2008 ('CCPR/C/103/D/1815/2008'), pp. 2 to 3, paras 2.1 to 2.3, , Available at: http://www.bayefsky.com/pdf/philippines_t5_ccpr_1815_2008_scan.pdf

119 CCPR/C/103/D/1815/2008, paras 9, 10. In December 2008, Adonis was released after nearly two years in prison. Centre for Media Freedom and Responsibility, 'Jailed broadcaster released', 28 December 2008, Available at: https://cmfr-phil.org/uncategorized/jailed-broadcaster-released/

the ICCPR, which requires all State parties to take steps to ensure domestic laws are in line with the Covenant.[120]

Notably, in contravention of the recommendations of the UN Human Rights Committee, a newer law was introduced in the Philippines to extend criminalization of defamation to the online sphere. The **Cybercrime Prevention Act of 2012 ('CPA')** not only extends this criminal offence to online expression or communication, but in fact increases the penalty for libel to nine years' imprisonment for libel committed online.[121] The Philippine Supreme Court has released guidelines on the imposition of penalties for libel cases which urge a "preference for the imposition of fine only rather than imprisonment in libel cases".[122] These guidelines do not have the force of law, however, and so do not preclude the imposition of an imprisonment sentence. They also apply only to certain select circumstances, and do not clarify that protection of the rights to free expression and information is a sufficient defence for libel.[123]

Myanmar

In Myanmar, section 66(d) of the **Telecommunications Law** ('section 66(d)') has been widely abused to impose criminal penalties on individuals who merely exercise their rights to free expression, opinion and information online, since its coming into force in 2013.

Section 66(d), as amended in August 2017, is a provision that is on its face not human rights compliant. It prohibits defamation of any person "using any telecommunications network" with a penalty of up to two years' imprisonment, a fine of up to 1mil. Kyat (approx. USD 652) or both.[124] Cases brought under section 66(d) by military officials have often, in recent times, been combined with charges under section 505(a) of Myanmar's **Penal**

120 CCPR/C/103/D/1815/2008, pp. 10, 11, paras 4 to 7; p.12.
121 See Section V below, for further analysis of the CPA. See also ICJ, 'Righting Wrongs: Criminal Law Provisions in the Philippines related to National Security and their Impact on Human Rights Defenders', pp. 17, 18, Available at: https://www.icj.org/wp-content/uploads/2015/03/Philippines-Criminal-Law-Provisions-Publications-Report-2015-ENG.pdf
122 Chief Justice Reynato S. Puno, 'Administrative Circular No. 08-2008: Guidelines in the Observance of a Rule of Preference in the Imposition of Penalties in Libel Cases', Available at: https://www.lawphil.net/courts/supreme/ac/ac_8_2008.html
123 Chief Justice Reynato S. Puno, 'Administrative Circular No. 08-2008: Guidelines in the Observance of a Rule of Preference in the Imposition of Penalties in Libel Cases', Available at: https://www.lawphil.net/courts/supreme/ac/ac_8_2008.html
124 English translation of Telecommunications Law (The Pyidaungsu Hluttaw Law No. 31, 2013) ('Telecommunications Law'), Available at: http://www.burmalibrary.org/docs23/2013-10-08-Telecommunications_Law-en.pdf; English translation of Amendment of Telecommunications Law (2017/ Pyi Htaung Su Hluttaw Law No.26), Available at: http://freeexpressionmyanmar.org/wp-content/uploads/2017/01/Telecommunications-Law-Amendment-EN.pdf

Code, which criminalizes the dissemination of information that could incite mutiny or otherwise cause members of the armed forces to disregard or fail in their duties (see below).[125]

As of April 2019, civil society organization Athan Myanmar documented that 185 cases had been formally filed under the Telecommunications Law, of which 93 percent invoked section 66(d), including 23 cases against 31 journalists.[126] In a 2018 analysis, Athan found that more than half of the cases filed under the Telecommunications Law – 54 percent –related to the exercise of free expression, including cases relating to political criticism and news reporting.[127] As of December 2017, civil society organization Free Expression Myanmar documented that half of the complainants who had filed cases against individuals under section 66(d) were representatives of the State or public officials.[128]

In a 2019 report, Athan noted that in the first six months of 2019 alone, 11 journalists had been charged for professional reporting – with 45 percent of charges brought against them under the Telecommunications Law and 15 percent brought under Myanmar's Penal Code for alleged criminal defamation.[129] Chapter XXI of Myanmar's **Penal Code** – sections 499 and 500 – criminalizes defamation with up to two years' imprisonment, a fine, or both.[130]

125 English translation of Myanmar Penal Code ('Myanmar Penal Code'), Available at: http://www.burmalibrary.org/docs6/MYANMAR_PENAL_CODE-corr.1.pdf

126 Athan Myanmar, ' The Number of Cases Under the Telecommunications Law', 9 April 2019, Available at: http://athanmyanmar.org/2019/04/09/the-number-of-cases-under-the-telecommunications-law/; Data from Say No to 66(d) campaign, Available at: https://www.saynoto66d.info/

127 Athan Myanmar, 'Mid-term report on Freedom of Expression', October 2018, Available at: https://equalitymyanmar.org/wp-content/uploads/2018/10/Mid-term-Report-on-Freedom-of-Expression-Eng-Version.pdf

128 Free Expression Myanmar, '66(d): No Real Change', December 2017, p17, Available at: http://freeexpressionmyanmar.org/wp-content/uploads/2017/12/66d-no-real-change.pdf

129 Athan Myanmar, '2019 Mid-year Report on Status of Freedom of Expression in Myanmar', Available at: https://progressivevoicemyanmar.org/2019/09/02/2019-mid-year-report-on-status-of-freedom-of-expression-in-myanmar/

130 The Electronic Transaction Law has also been used to control online content. See ICJ, ' Myanmar: Briefing Paper on Criminal Defamation Laws', 26 November 2015, Available at: https://www.icj.org/wp-content/uploads/2015/11/Myanmar-Criminal-Defamation-Laws-Advocacy-Position-paper-2015-ENG.pdf

Case of ***Ko Swe Win***

In July 2017, **Ko Swe Win**, editor-in-chief of news outlet Myanmar Now, was arrested following the filing of a complaint by a member of ultra-nationalist group Ma Ba Tha that he had allegedly defamed U Wirathu, a Buddhist monk and former leader of the group.[131]

The complaint was filed under section 66(d) in March 2017, following a post Ko Swe Win had made on his Facebook page that alleged that U Wirathu had 'violated' the rules of monkhood. In February 2017, U Wirathu had praised – in a Facebook post – the killer of human rights lawyer U Ko Ni, who was assassinated following his vocal advocacy against hate speech and racial and religious discrimination.[132]

Soon after, Myanmar Now reported on U Wirathu's post, including a quote from a senior monk who alleged that U Wirathu's comments could warrant expulsion from monkhood.[133] Ko Swe Win's Facebook post referred to the Myanmar Now article.

From the time his trial commenced in July 2017, Ko Swe Win travelled long distances between the court in Mandalay where charges against him were filed and his home in Yangon for nearly two years to attend more than 55 hearings.[134] Each round-trip took him a minimum of 16 hours and cost him at least 500,000 Kyats (approx. USD 330).[135]

Multiple irregularities were observed in the trial process, including constant delays by the plaintiff resulting in unreasonable prolonging of his trial, in contravention of his fair trial rights.

In July 2019, after two years, the court in Mandalay dropped the case against Ko Swe Win.[136]

131 Sean Gleeson, 'Myanmar Now editor Ko Swe Win arrested at Yangon Airport', *Frontier Myanmar,* 30 July 2017, Available at: https://frontiermyanmar.net/en/myanmar-now-editor-ko-swe-win-arrested-at-yangon-airport

132 ICJ, 'Myanmar: ICJ marks 2nd year anniversary of the killing of lawyer U Ko Ni', 29 January 2018, Available at: https://www.icj.org/myanmar-icj-marks-2nd-year-anniversary-of-the-killing-of-lawyer-u-ko-ni/; ICJ, 'Killing of lawyer U Ko Ni must be promptly and impartially investigated', 30 January 2017, Available at: https://www.icj.org/icj-statement-on-the-killing-of-lawyer-u-ko-ni/

133 Htun Khaing, 'Prominent reporter refuses to apologise after Ma Ba Tha files defamation suit', *Frontier Myanmar,* 8 March 2017, Available at: https://frontiermyanmar.net/en/prominent-reporter-refuses-to-apologise-after-ma-ba-tha-files-defamation-suit

134 ICJ et. al, 'Joint statement: Myanmar authorities must drop the case against Ko Swe Win and decriminalise defamation', 7 March 2019, Available at: https://www.icj.org/joint-statement-myanmar-authorities-must-drop-the-case-against-ko-swe-win-and-decriminalise-defamation/

135 Moe Myint, 'Nationalists Subject Journalist to Devastating Legal Ordeal', *The Irrawaddy,* 17 January 2019, Available at: https://www.irrawaddy.com/features/nationalists-subject-journalist-devastating-legal-ordeal.html

136 Zarni Mann, 'Lawsuit Against Myanmar Now Editor Dropped After 2 Years', *The Irrawaddy,* 2 July 2019, Available at: https://www.irrawaddy.com/news/burma/lawsuit-myanmar-now-editor-dropped-2-years.html

Case of ***Min Htin Ko Ko Gyi***

In April 2019, **Min Htin Ko Ko Gyi**, filmmaker and founder of a human rights film festival in Myanmar, was arrested and taken into pre-trial detention following a complaint filed against him under section 66(d) for alleged defamation of the military regarding posts he had made on Facebook criticizing the role of the military in Myanmar's politics.[137]

Lt. Col. Lin Htun of Yangon Regional Command filed the case against the filmmaker, and a second case for alleged violation of section 505(a) of Myanmar's Penal Code.[138]

Min Htin Ko Ko Gyi remained in prison, despite requiring access to medical treatment as he suffers from liver cancer and underwent a serious operation prior to his arrest and detention.[139]

In August 2019, he was convicted of the charge under section 505(a) of the Penal Code and sentenced to one year in prison with hard labour.[140]

In a similar case:

In May 2016, poet **Maung Saung Kha** was convicted under section 66(d) and sentenced to six months' imprisonment for alleged defamation of former president Thein Sein following a poem he posted on Facebook in October 2015.[141]

137 San Yamin Aung, 'Filmmaker Accused of Insulting Army Is Denied Bail, Sent to Prison', *The Irrawaddy,* 12 April 2019, Available at: https://www.irrawaddy.com/news/burma/filmmaker-accused-insulting-army-denied-bail-sent-prison.html

138 Section 505(a) of the Penal Code is a non-bailable offence, where a judge can make a decision to grant bail to the accused.

139 Amnesty International, 'Myanmar: Health Concerns For Detained Filmmaker: Min Htin Ko Ko Gyi', 6 June 2019, Available at: https://www.amnesty.org/en/documents/asa16/0478/2019/en/

140 Sam Aung Moon, 'Myanmar jails filmmaker for Facebook posts critical of military', *Reuters,* 29 August 2019, Available at: https://www.reuters.com/article/us-myanmar-filmmaker/myanmar-jails-filmmaker-for-facebook-posts-critical-of-military-idUSKCN1VJ0Q5?feedType=RSS&feedName=worldNews

141 PEN International, 'Myanmar: Poet sentenced to 6 months in prison and released', 25 May 2016, Available at: https://www.pen-international.org/news/myanmar-poet-sentenced-to-6-months-in-prison-and-released

Case of ***Peacock Generation Thangyat group***

In April 2019, members of the **Peacock Generation (Daungdoh Myoset) *thangyat* group** – a performance art group that does traditional slam poetry – were charged under section 66(d) and section 505(a) of the Penal Code after Lt. Col. Than Tun Myint of Yangon Regional Command filed a complaint against them for alleged defamation of the military following a satirical arts performance which the group had live-streamed on Facebook.[142]

In October 2019, a court in Yangon's Mayangone township sentenced Kay Khine Tun, Zayar Lwin, Paing Ye Thu, Paing Phyo Min, and Zaw Lin Htut each to one year in prison with hard labour for violation of section 505(a) of the Penal Code. [143] They had been held in pre-trial detention since April when they were denied bail.[144]

In November 2019, a court in Yangon's Botataung township sentenced the same five and a sixth member, Su Yadanar Myint, to a year in prison for violation of section 505(a) of the Penal Code, increasing the imprisonment term of the earlier five to two years.[145]

Zayar Lwin, Paing Ye Thu and Paing Phyo Min face further charges under 505(a) in three other township courts, in apparent violation of the fair trial principle of *non bis in idem,*[146]and all six members along with a seventh, Nyein Chan Soe, face charges under section 66(d) for alleged defamation of the military.[147]

142 Htet Arkar, Roseanne Gerin, 'Myanmar Satire Troupe Denied Bail, Remanded to Insein Prison For Lampooning Military', *Radio Free Asia*, 22 April 2019, Available at: https://www.rfa.org/english/news/myanmar/myanmar-satire-troupe-denied-bail-04222019164338.html

143 Zaw Zaw Htwe, 'Five Members of Performance Troupe Jailed for Satirizing Myanmar Military', *The Irrawaddy*, 30 October 2019, Available at: https://www.irrawaddy.com/news/burma/five-members-performance-troupe-jailed-satirizing-myanmar-military.html; Human Rights Watch, 'Myanmar: Actors Convicted of Criticizing Army', 31 October 2019 ('HRW, 31 October 2019'), Available at: https://www.hrw.org/news/2019/10/31/myanmar-actors-convicted-criticizing-army

144 Htet Arkar, Roseanne Gerin, 'Myanmar Satire Troupe Denied Bail, Remanded to Insein Prison For Lampooning Military', *Radio Free Asia*, 22 April 2019, Available at: https://www.rfa.org/english/news/myanmar/myanmar-satire-troupe-denied-bail-04222019164338.html

145 Human Rights Watch, 'Myanmar: More Jail Time for Satirical Troupe', 19 November 2019 ('HRW, 19 November 2019'), Available at: https://www.hrw.org/news/2019/11/19/myanmar-more-jail-time-satirical-troupe

146 The fair trial principle of *non bis in idem* ensures that an individual who has been tried and punished for an offence is not tried or punished for a second time in criminal proceedings in the same jurisdiction.

147 HRW, 31 October 2019; HRW, 19 November 2019.

Thailand

In Thailand, criminal defamation provisions in the **Criminal Code**, in themselves not human rights compliant, have been abused to clamp down on persons seeking to bring to public attention information regarding human rights violations.[148] Criminal defamation under sections 326 and 327 of the Criminal Code carry a maximum sentence of one year's imprisonment, a fine of up to 20,000 Baht (approx. USD 640) or both, while section 328 criminalizes defamation "by means of publication" with up to two years' imprisonment and a fine of up to 200,000 Baht (approx. USD 6,400).[149]

The **Computer-related Crimes Act B.E. 2560 (2017)** ('CCA') – as amended from its 2007 version – has often been used alongside criminal defamation provisions to extend criminalization to expression and information online. Section 14(2) of the CCA criminalizes the "entering of false computer data" which is "likely to cause damage to the protection of national security, public safety… or cause panic to the public", while section 14(3) criminalizes any such "false" data entry which is "an offence against the security of the Kingdom or is an offence relating to terrorism". Both crimes are punishable with up to five years' imprisonment, a fine of up to 100,000 Baht (approx. USD 3,200), or both.[150] As will be shown below, the CCA has also been used alongside lesè majesté provisions in Thai law to curtail online speech relating to the monarchy.

The ICJ has consistently called for the repeal or amendment of articles 326 to 328 of the Criminal Code and section 14 of the CCA in line with Thailand's international human rights obligations, including under the ICCPR to which Thailand is a State party.[151] Though article 14(1) of the CCA was amended in 2017 to explicitly state that the sub-provision does not

148 ICJ has called for Thailand's criminal defamation laws to be repealed or amended in line with Thailand's international legal obligations. See for eg. ICJ, 'Thailand: misuse of laws restricts fundamental freedoms (UN statement)', 14 March 2018, Available at: https://www.icj.org/hrc37thailand/; ICJ, 'Thailand: verdict in Andy Hall case underscores need for defamation to be decriminalized', 20 September 2016, Available at: https://www.icj.org/thailand-verdict-in-andy-hall-case-underscores-need-for-defamation-to-be-decriminalized/; ICJ, 'Thailand: end prosecution of Phuketwan journalists and repeal criminal defamation laws', 1 September 2015, Available at: https://www.icj.org/thailand-end-prosecution-of-phuketwan-journalists-and-repeal-criminal-defamation-laws/

149 English translation of Thai Criminal Code B.E. 2499 ('Thai Criminal Code'), Available at: https://www.thailandlawonline.com/laws-in-thailand/thailand-criminal-law-text-translation#326

150 English translation of Computer-related Crimes Act B.E. 2560 ('Thai Netizen, CCA'), Available at: https://thainetizen.org/docs/cybercrime-act-2017/

151 ICJ, TLHR, 'Joint Submission of the International Commission of Jurists and Thai Lawyers for Human Rights in advance of the examination of the Kingdom Of Thailand's Second Periodic Report under Article 40 of the International Covenant on Civil And Political Rights', 6 February 2017, Available at: https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/THA/INT_CCPR_CSS_THA_26602_E.pdf

apply to "defamation offences as under the Criminal Code",[152] in practice, articles 14(2) and 14(3) have been used to suppress free expression online.[153]

It is not only State actors, but also companies who have increasingly wielded defamation complaints to silence individuals attempting to bring to light human rights violations. In two cases relating to criminal and civil defamation proceedings launched by companies – namely Natural Fruit Company Ltd. and Thammakaset Co. Ltd. – against human rights defenders and researchers who had alleged labour rights violations by the companies, the ICJ, along with Lawyers' Rights Watch Canada, made *amicus curiae* submissions. These submissions argued that all branches of government, including the judiciary, have obligations to protect individuals from acts by private persons or entities – including companies – which curtail free expression and opinion, and that criminal sanctions for defamation in particular would contravene the right to free expression and opinion.[154]

Regrettably, following a preliminary hearing of the case involving Thammakaset Co. Ltd in 2019 (see below), the Bangkok Criminal Court responded to the ICJ's *amicus curiae* submission by ruling that Thailand's criminal defamation laws did not violate Thailand's international human rights obligations under the ICCPR.[155] The Court, in its decision, appeared to endorse criminal penalties as a suitable remedy to address the repercussions of allegedly defamatory speech, and failed to view reporting on labour rights violations allegedly committed by a corporation as a matter of public interest.[156] In retaining legal provisions that allow private companies to bring criminal defamation complaints against individuals seeking to bring to light human rights violations, the Thai government has failed to uphold its obligations in line with the UNGPs to provide effective access to remedy for victims of such violations.

152 Thai Netizen, CCA.

153 Article 14(2) was, for example, used in the case of *Manager Online* below and article 14(3) has been used more in cases relating to lesè majesté.

154 ICJ, LRWC, 'Amicus Curiae Brief in the case of the defendant Andy Hall (Black Case Number A 517/2556)', July 2016, Available at: https://www.icj.org/thailand-amicus-in-criminal-defamation-proceedings-against-human-rights-defender-andy-hall/; ICJ, LRWC, 'Amicus Curiae Brief in the case of the defendant Mr. Nan Win (Black Case Number Aor.3011/2561) and Ms. Sutharee Wannasiri (Black Case Number Aor. 3054/2561)', January 2019, Available at: https://www.icj.org/thailand-icj-and-lrwc-submit-amicus-in-criminal-defamation-proceedings-against-human-rights-defenders-nan-win-and-sutharee-wannasiri/

155 This was a regrettable decision, even as the ruling was an interesting departure from usual practice by Thai courts who do not often respond substantially to arguments put forth on the basis of international law. The court, in this case, addressed the 'three-part' test under article 19 in deciding that Thailand's criminal defamation laws were in line with the ICCPR.

156 The court, for example, opined that criminal penalties for defamation were justified in the context of Thailand as the dissemination of incorrect information about a person could cause him or her to lose their job, affect his or her or their family's security.

Case of ***Isma-ae Tae***

In February 2018, **Isma-ae Tae**, a human rights defender from Thailand's southern border provinces and founder of Patani Human Rights Organization, had a complaint lodged against him for criminal defamation by a Director of the Internal Operations Security Command (ISOC) in Thailand's military.[157] He was thereafter charged by the police.

The accusations related to a TV programme that had aired on 5 February 2018 in which Tae had described being tortured and ill-treated by soldiers in 2008.

In October 2016, Thailand's Supreme Administrative Court had ordered the Royal Thai Army and Ministry of Defence to pay 305,000 Baht (approx. USD 9,700) in compensation to Tae, after it found he had been "physically assaulted" during detention and detained illegally for nine days – exceeding the limit of seven days permitted under Thai Martial Law.[158]

In a similar case:

In November 2017, **Anuphong Phanthachayangkun**, a former Sub-district Head from Narathiwat province, was sentenced to one year in prison after the police filed a criminal defamation complaint against him for filing a complaint against 20 police officers for allegedly subjecting him to torture leading to a "confession" in relation to a 2004 case.[159]

157 ISOC is responsible for security operations in Thailand's restive Southern Border Provinces.
158 ICJ, 'Thailand: immediately stop criminal defamation complaint against torture victim', 15 February 2018, Available at: https://www.icj.org/wp-content/uploads/2018/02/Thailand-Isma-ae-Tae-defamation-case-News-Press-releases-2018-ENG.pdf
159 ICJ, 'Thailand: immediately stop criminal defamation complaint against torture victim', 15 February 2018, Available at: https://www.icj.org/wp-content/uploads/2018/02/Thailand-Isma-ae-Tae-defamation-case-News-Press-releases-2018-ENG.pdf

Case of ***Manager Online***

In February 2018, the **editor of 'Manager Online'** news website faced charges under section 328 of the Criminal Code and section 14(2) of the CCA, after a Director of Thailand's ISOC authorized the filing of a criminal defamation complaint against him.

This followed the publication of a story on the website on 5 February 2018 which had alleged torture and ill-treatment of a suspect in military camps. The military further sought 10 mil. Baht (approx. USD 320,000) in damages from the news website for its report.[160]

In February 2019, the ICJ was informed that complaints against the editor and a second editor of the same website had been withdrawn, following a settlement obliging 'Manager Online' to publish a "clarification statement" drafted by ISOC Region 4 Forward division, which had brought the criminal defamation charges against them. The statement indicated that "after examining all facts", the editors had found "it is not true" and expressed "remorse about (our) wrongdoing by publishing an article that defamed officers of the ISOC 4 Forward, and damaged their reputation." The statement urged all groups "to stop bringing security problems in the region to defame the officers for their own benefit or their political interests and to stop deceiving the public with distorted information."[161]

In a submission to the UN Human Rights Committee in April 2019, the ICJ highlighted that this settlement had done nothing to allay concerns that criminal defamation charges had been used to legally harass and threaten the news website in the first place.[162]

160 ICJ, 'Thailand: immediately stop criminal defamation complaint against torture victim', 15 February 2018, Available at: https://www.icj.org/wp-content/uploads/2018/02/Thailand-Isma-ae-Tae-defamation-case-News-Press-releases-2018-ENG.pdf

161 Manager Online, "Clarification Statement," 14 February 2019, Available at: https://mgronline.com/south/detail/9620000015540

162 ICJ, TLHR, CrCF, 'Supplementary Submission by the International Commission of Jurists, Thai Lawyers For Human Rights and Cross-Cultural Foundation on Thailand's Implementation of the Human Rights Committee's Prioritized Recommendations following its Review of Thailand's Second Periodic Report at its 119th Session', April 2019, para 20.

Cases of ***Nan Win, Sutharee Wannasiri*** and others

In October 2018, Thammakaset Co. Ltd. filed a criminal defamation suit under sections 326 and 328 of the Criminal Code against **Sutharee Wannasiri**, human rights defender and a former Thailand Human Rights Specialist with non-governmental organization Fortify Rights, for three comments she was alleged to have made on Twitter related to a film produced by Fortify Rights.[163]

The film, published in October 2017, had called on Thai authorities to drop existing criminal defamation charges against 14 migrant workers at a Thammakaset-operated chicken farm and to decriminalize defamation in Thailand. These charges had been brought against the migrant workers for alleging labour rights violations committed by the company.

In October 2018, Thammakaset Co. Ltd. filed a criminal defamation suit under sections 326 and 328 of the Criminal Code against **Nan Win**, one of the 14 migrant workers from Myanmar, for two interviews he gave in a Fortify Rights film and during a Fortify Rights press conference on 6 October 2017.

Thammakaset Co. Ltd. also filed a civil defamation suit against Sutharee Wannasiri citing the above-mentioned Twitter comments and demanding five million Thai Baht (more than USD 142,000) in compensation for alleged damage to the company's reputation.

In related cases:

Other cases brought by the company against any individuals perceived to have expressed dissent, conducted advocacy on or released information relating to labour rights violations committed by Thammakaset Co. Ltd. included criminal defamation complaints under articles 326 and 328 of the Criminal Code against:

Ngamsuk Rattanasatiean, who had shared information on the Facebook page of the Institute of Human Rights and Peace Studies;

Suchanee Rungmuanporn, a former reporter from Voice TV who had made a post on Twitter highlighting labour rights violations by Thammakaset;

Suthasinee Kaewleklai, coordinator of the Migrant Workers Rights

163 ICJ et. al, 'Thailand: Drop defamation complaints against human rights defenders Nan Win and Sutharee Wannasiri', 3 December 2018, Available at: https://www.icj.org/thailand-drop-defamation-complaints-against-human-rights-defenders-nan-win-and-sutharee-wannasiri/

Network, who had shared information on Facebook relating to the cases;

and other separate cases against Nan Win, other migrant workers and Sutharee Wannasiri.[164]

Case of ***Angkhana Neelapaijit***

In November 2019, **Angkhana Neelapaijit**, former National Human Rights Commissioner of Thailand and a recipient of the Ramon Magsaysay Award in 2019, was served with a court warrant following the filing of a defamation suit against her by Thammakaset Co. Ltd. under sections 326 and 328 of the Criminal Code. The suit alleged harm from two posts she had made on Twitter, where she had shared links to press statements by civil society referring to the case of Sutharee Wannasiri, Nan Win and other migrant workers.

The first Twitter post in question was a re-Tweet by Angkhana Neelapaijit in December 2018 to the ICJ website which had a link to a joint statement co-signed by the ICJ and 15 other organizations, calling on Thammakaset Co. Ltd. to cease legal harassment of individuals for bringing to light labour violations. The second Twitter post in June 2019 had shared a link to a news release by the NGO Fortify Rights.

Both posts had allegedly contained a link to the film by Fortify Rights which had been the subject of the suits against Sutharee Wannasiri, Nan Win and others. Thammakaset Co. Ltd. argued that her Twitter posts had, in 'sharing' weblinks to statements which contained weblinks to the film, violated criminal defamation laws.

In February 2020, a "conciliation conference" is expected to be held in this case against the former National Human Rights Commissioner.[165]

164 Information from ICJ partners. See also FIDH, OMCT, 'Thailand: FACT SHEET Thammakaset vs. human rights defenders and workers in Thailand', May 2019, Available at: https://www.fidh.org/IMG/pdf/obsthailande2019web.pdf

165 ICJ, 'Thailand: ICJ condemns the use of criminal defamation law to harass Angkhana Neelapaijit', 27 November 2019, Available at: https://www.icj.org/thailand-icj-condemns-the-use-of-criminal-defamation-law-to-harass-angkhana-neelapaijit/

Indonesia

In Indonesia, defamation provisions in the **Penal Code** and the **Law on Electronic Information and Transactions (Law No. 11 of 2008)** ('UU ITE'), in themselves not human rights compliant, have been applied in practice by State authorities to impermissibly limit freedom of expression and information online.[166]

Chapter XVI of Indonesia's Penal Code, including sections 310 to 321, criminalizes defamation with up to four years' imprisonment and a maximum fine of 300 Rupiah (approx. USD 0.02). Sections 310 and 311 allow for a maximum punishment of 16 months' imprisonment for "intentionally harming a person's reputation" to be increased to four years' imprisonment where the accused person fails to prove truth as a defence. Section 316 allows for punishments to be "enhanced with a third" for alleged defamation against an official "during or on the subject of the legal exercise of his office".[167] Pending draft amendments to the Penal Code raise further concerns that criminal defamation may be extended to insults against the President or Vice President, insults against Islam and public insults against "general authority or state institutions". Contempt of court penalties of between one to five years' imprisonment are also problematic.[168] The draft amendments also contain provisions allowing for criminal penalties to be brought against a person for spreading "hoax news".[169]

In 2008, the UU ITE was passed, and thereafter revised in 2016, to regulate electronic information and transactions, including criminal penalties for online defamation of up to four years' imprisonment and/or a maximum fine of 1 bil. Rupiah (approx. USD 52,300), and up to 12 years' imprisonment

166 ICJ has called for Thailand's criminal defamation laws to be repealed or amended in line with Thailand's international legal obligations. See for eg. ICJ, 'Thailand: misuse of laws restricts fundamental freedoms (UN statement)', 14 March 2018, Available at: https://www.icj.org/hrc37thailand/; ICJ, 'Thailand: verdict in Andy Hall case underscores need for defamation to be decriminalized', 20 September 2016, Available at: https://www.icj.org/thailand-verdict-in-andy-hall-case-underscores-need-for-defamation-to-be-decriminalized/; ICJ, 'Thailand: end prosecution of Phuketwan journalists and repeal criminal defamation laws', 1 September 2015, Available at: https://www.icj.org/thailand-end-prosecution-of-phuketwan-journalists-and-repeal-criminal-defamation-laws/

167 English translation of Penal Code of Indonesia, Available at: https://www.oecd.org/site/adboecdanti-corruptioninitiative/46814438.pdf

168 Kate Walton, 'Indonesia's Criminal Code revisions: politics or religion?', *New Naratif,* 8 February 2018, Available at: https://newnaratif.com/journalism/indonesias-criminal-code-revisions-politics-religion/

169 [Bahasa Indonesia] M Rosseno Aji, 'Ini 10 Pasal RKUHP yang ancam Kebebasan Pers menurut LBH Pers', Available at: https://nasional.tempo.co/read/1250897/ini-10-pasal-rkuhp-yang-ancam-kebebasan-pers-menurut-lbh-pers/full&view=ok; [Bahasa Indonesia] Scholastica Gerintya, 'Periksa Data- Jerat UU ITE Banyak Dipakai oleh Pejabat Negara', 18 October 2018, Available at: https://tirto.id/jerat-uu-ite-banyak-dipakai-oleh-pejabat-negara-c7sk

and/or a maximum fine of 2 bil. Rupiah (approx. USD 140,000) where the alleged online defamatory act causes harm to others.[170] As of October 2018, 245 complaints had reportedly been brought under the UU ITE, with public officers and government agencies comprising 35.92 percent of the complainants.[171] As of January 2019, only 6 percent of indicted cases had reportedly been acquitted.[172]

Case of ***Anindya Shabrina Joediono***

In August 2018, **Anindya Shabrina Joediono**, a law student from Surabaya and editor-in-chief of online news platform 'Merah Muda Memudar', received a warrant to report for investigation following a complaint that had been filed against her under sections 27(3) and 45(3) of the UU ITE, by a person who alleged she had defamed the police, including the municipal police of Surabaya.

This came after she had made a Facebook post and a comment on a YouTube video alleging sexual assault by police officers following a film screening and discussion on human rights violations which they had entered to shut down.[173]

As of January 2019, Joediono reportedly remains under police investigation.[174]

170 See in particular Articles 27(3), 29, 45(1), 45(3). English translation of Law of the Republic of Indonesia No. 11 of 2008 Concerning Electronic Information and Transactions, Available at: http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html; On the 2016 amendments, see for eg. Institute for Criminal Justice Reform, 'Response to the Revision of Information and Electronic Transaction Law (ITE Law): Five Crucial Issues in the ITE Law that Threaten Freedom of Expression in Indonesia', 28 October 2016, Available at: https://icjr.or.id/response-to-the-revision-of-information-and-electronic-transaction-law-ite-law-five-crucial-issues-in-the-ite-law-that-threaten-freedom-of-expression-in-indonesia/

171 [Bahasa Indonesia] Scholastica Gerintya, 'Periksa Data- Jerat UU ITE Banyak Dipakai oleh Pejabat Negara', 18 October 2018, Available at: https://tirto.id/jerat-uu-ite-banyak-dipakai-oleh-pejabat-negara-c7sk

172 Johannes Nugroho, Charis Loke, 'Silenced by an Elastic Law', *New Naratif,* 4 January 2019 ('*New Naratif,* 4 January 2019'), Available at: https://newnaratif.com/journalism/silenced-by-an-elastic law/share/pybxr/259dff62034ffb4223adcb949a50f667/

173 *New Naratif,* 4 January 2019; Palang Hitam Indonesia, 'Solidarity with Anindya Shabrina', 6 September 2018, Available at: https://palanghitam.noblogs.org/anindya-shabrina/

174 *New Naratif,* 4 January 2019.

Case of ***Jakarta Globe, Okezone.com*** and ***Harian Bangsa***

In April 2009, the Police Chief of East Java, Chief Insp. Gen. Anton Bachrul Alam announced that criminal defamation complaints had been filed under sections 310 and 311 of the Penal Code against news outlets ***Jakarta Globe, Okezone.com*** and ***Harian Bangsa*** following articles they had published online which had reported on an election complaint filed that day.

The complaint had been filed with electoral authorities alleging that politician Edhi Baskoro Yudhoyono had been involved in election vote-buying. The complaints filed against the news outlets were lodged on the basis that the outlets had, in reporting on the election complaint, defamed Edhi himself.[175]

The police chief thereafter announced charges had been dropped. One journalist noted how this experience showed that even in cases in which journalists had discharged their duties professionally and without bias, "because of this defamation law, we can still be brought to court."[176]

Singapore

In Singapore, **civil defamation** lawsuits have long been invoked by representatives of the ruling People's Action Party (PAP) – including by former Prime Ministers Lee Kuan Yew and Goh Chok Tong and current Prime Minister Lee Hsien Loong – to sue and seek hefty financial compensation in terms of damages from individuals who express dissent.[177] The systematic use of these civil actions since the 1970s has resulted in curtailment of free expression through the imposition of heavy financial burdens or outright bankrupting of members of the political opposition, independent journalists, local or international news outlets and ordinary individuals.[178] In recent

175 Mail & Guardian, 'Indonesian president's son in vote-buying row', 20 November 2019, Available at: https://mg.co.za/article/2009-04-08-indonesian-presidents-son-in-votebuying-row

176 Human Rights Watch, 'Turning Critics into Criminals – The Human Rights Consequences of Criminal Defamation Law in Indonesia', 2010, pp. 31, 32, Available at: https://www.hrw.org/sites/default/files/reports/indonesia0510webwcover.pdf

177 For a single defamation suit, the Prime Minister has been awarded up to S$500,000 in damages and Members of Parliament have been awarded up to S$210,000 in damages. See Po Jen Yap, *Constitutional Dialogue in Common Law*, p. 117, footnote 64; See also Tsun Hang Tey, 'Singapore's jurisprudence of political defamation and its triple-whammy impact on political speech', 2008, *Public Law*, pp. 452 to 462 ('Tsun Hang Tey, 2008'; Cameron Sim, 'The Singapore Chill: Political Defamation and the Normalization of a Statist Rule of Law', 2011, *Pacific Rim Law & Policy Journal, Vol. 20(2)*, pp. 319 to 353.

178 Tsun Hang Tey, 2008, pp. 452, 453, referring, inter alia, to *Jeyaretnam JB v Lee Kuan Yew* [1978-1979] Sing.L.R. 197; [1979] SGCA 13; [1979] 2 MLJ 282; *Lee Hsien Loong v Singapore*

years, along with civil suits, criminal defamation laws have been wielded against independent bloggers or news websites to censor content online.[179]

Sections 499 and 500 of Singapore's **Penal Code** criminalizes defamation with up to two years' imprisonment or a fine or both.[180] Civil actions for defamation are brought in line with the common law doctrine of torts and the Defamation Act.[181]

Case of ***Roy Ngerng***

In December 2015, independent blogger **Roy Ngerng** was ordered to pay S$150,000 in damages (approx. USD 109,700) for alleged defamation of Prime Minister Lee Hsien Loong in relation to an article he had published in May 2014 on his blog, questioning the government's management of the Central Provident Fund.[182] He had also posted a link to his article on his Facebook page and the Facebook page of his blog.

This decision came after solicitors representing the Prime Minister sent a letter in May 2014 to Ngerng demanding that he remove the blog article and Facebook posts and publish an apology. Ngerng removed the article a few days later and sent a letter of apology to the lawyers.[183]

In June 2015, the ICJ submitted a Legal Opinion in Ngerng's case, expressing concern that "a decision awarding a disproportionately high amount of damages to the plaintiff… would cast a chilling effect on freedom of expression in Singapore."[184]

Democratic Party [2007] 1 Sing.L.R. 675; [2006] SGHC 220; See Jothie Rajah, 'Authoritarian Rule of Law: Legislation, Discourse and Legitimacy in Singapore', 2012; See also, for an example of how international media outlets have been subject to civil defamation actions, Reuters, 'New York Times pays damages to Singapore's leaders', 24 March 2010, Available at: https://www.reuters.com/article/us-singapore-newyorktimes/new-york-times-pays-damages-to-singapores-leaders-idUSTRE62N26D20100324

179 Human Rights Watch, '"Kill the Chicken to Scare the Monkeys" - Suppression of Free Expression and Assembly in Singapore', 12 December 2017, Available at: https://www.hrw.org/report/2017/12/12/kill-chicken-scare-monkeys/suppression-free-expression-and-assembly-singapore

180 Penal Code (Chapter 224) Rev. Ed. 2008, Available at: https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr500-#pr500-

181 Defamation Act (Chapter 75) Rev. Ed. 2014, Available at: https://sso.agc.gov.sg/Act/DA1957#pr10-

182 The Central Provident Fund is a State-run mandatory social security savings scheme.

183 See *Lee Hsien Loong v Roy Ngerng Yi Ling* [2015] SGHC 320, Available at: file:///C:/Users/User/Desktop/RoyNgerng%202015-SGHC-320.pdf

184 ICJ, 'Legal Opinion supporting the case of the Defendant in Lee Hsien Loong (Prime Minister of Singapore) v Roy Ngerng Yi Ling – Suit No. 569/2014', 23 June 2015, Available at: https://www.icj.org/wp-content/uploads/2015/07/Singapore-RoyNgerng-Advocacy-LegalOpinion-2015-ENG-.pdf

Case of ***The Online Citizen*** **(i)**

In December 2018, **Terry Xu**, editor of independent news website The Online Citizen (TOC), and **Daniel De Costa**, author of a letter posted on TOC, were charged with criminal defamation for an article posted on TOC's website which had alleged "corruption at the highest echelons" within the Singapore government.[185]

The charges under sections 499 and 500 of the Penal Code were made on the basis that the allegation was made with knowledge that "such imputation would harm the reputation of the members of the Cabinet of Singapore".[186] De Costa was also charged under the Computer Misuse Act for unauthorized access to an email account, which he had reportedly used without the individual's consent to communicate the article.[187]

In November 2018, police searched the homes of Xu, De Costa and a third individual named 'Willy Sum' and seized electronic equipment. Terry Xu and 'Willy Sum' were also brought into the police station for questioning.[188]

De Costa's constitutional challenge against the criminal defamation charge against him is due to be heard on 27 November 2019. The challenge concerns the question of whether the phrase "the reputation of such person" under section 499 of the Penal Code should read to be limited to "natural persons" alone, and cannot be extended to the Cabinet.[189]

185 Shaffiq Alkhatib, 'TOC editor Terry Xu and alleged contributor to site charged with criminal defamation', *Straits Times*, 13 December 2018, Available at: https://www.straitstimes.com/singapore/courts-crime/toc-editor-terry-xu-and-alleged-contributor-to-site-charged-with-criminal

186 Coconuts Singapore, 'The Online Citizen editor Terry Xu charged for defaming Cabinet of Singapore members', 12 December 2018, Available at: https://coconuts.co/singapore/news/online-citizen-editor-terry-xu-charged-defaming-cabinet-singapore-members/

187 Shaffiq Alkhatib, 'TOC editor Terry Xu and alleged contributor to site charged with criminal defamation', *Straits Times*, 13 December 2018, Available at: https://www.straitstimes.com/singapore/courts-crime/toc-editor-terry-xu-and-alleged-contributor-to-site-charged-with-criminal

188 Coconuts Singapore, 'The Online Citizen editor Terry Xu charged for defaming Cabinet of Singapore members', 12 December 2018, Available at: https://coconuts.co/singapore/news/online-citizen-editor-terry-xu-charged-defaming-cabinet-singapore-members/

189 Kathleen F., 'Court to hear Daniel de Costa's constitutional challenge in criminal defamation charge on 27 November', *The Online Citizen,* 12 September 2019, Available at: https://www.theonlinecitizen.com/2019/09/12/court-to-hear-daniel-de-costas-constitutional-challenge-in-criminal-defamation-charge-on-27-november/

Case of ***The Online Citizen*** **(ii)**

In September 2019, **Terry Xu** was served with a writ by lawyers representing Prime Minister Lee Hsien Loong commencing criminal defamation proceedings against him for publishing an article on TOC in August 2019 titled "PM Lee's wife Ho Ching weirdly shares article on cutting ties with family members".[190]

The article had referred to a post made on Facebook by the Prime Minister's wife and reported on a public feud between members of the Prime Minister's family.

Prior to the commencement of the suit, the Press Secretary to the Prime Minister had submitted a letter to Xu requesting that he remove the article and a Facebook post including a link to the article, and publish "a full and unconditional apology, plus an undertaking not to publish any similar allegations, prominently on your website and on your Facebook timeline".[191]

The first pre-trial conference was held on 15 October.[192]

ii. Laws which aim to protect the reputation of the monarchy

Laws which aim to protect the reputation of the monarchy, particularly through *lèse majesté* provisions, have also been wielded to control free expression and information on online platforms. This section examines the misuse of such laws in *Thailand, Cambodia* and *Malaysia*. *Thailand* provides the most dramatic example of misuse to restrict free expression of opinions. Similar legislation recently introduced in *Cambodia* was closely based on the Thai model. *Malaysia*, in contrast, does not have *lèse majesté* laws *per se* but have utilized laws restricting sedition to prosecute alleged critics of the monarchy.

190 Louisa Tang, 'TOC article 'gravely injured' PM Lee's character and reputation, say lawyers seeking aggravated damages in defamation suit', *Today Online,* 6 September 2019, Available at: https://www.todayonline.com/singapore/toc-article-gravely-injured-pm-lees-character-and-reputation-say-lawyers-seeking

191 The letter further argued that action by the Prime Minister was required to "rebut and deal publicly with such scurrilous attacks on his integrity and character, if necessary through legal action". Kenneth Cheng, 'PM Lee demands The Online Citizen take down allegedly defamatory article or face legal action', *Today Online,* 1 September 2019, Available at: https://www.todayonline.com/singapore/pm-lee-demands-editor-online-citizen-remove-defamatory-article-or-face-legal-action

192 Coconuts Singapore, 'The Online Citizen editor Terry Xu charged for defaming Cabinet of Singapore members', 12 December 2018, Available at: https://coconuts.co/singapore/news/online-citizen-editor-terry-xu-charged-defaming-cabinet-singapore-members/

In clarifying the scope of State obligations to respect and protect freedom of expression under the ICCPR, the UN Human Rights Committee has expressed concern that *lèse majesté* laws may unduly restrict public debate:

"(T)he mere fact that forms of expression are considered to be insulting to a public figure is not sufficient to justify the imposition of penalties, albeit public figures may also benefit from the provisions of the Covenant. Moreover, all public figures, including those exercising the highest political authority such as heads of state and government, are legitimately subject to criticism and political opposition. Accordingly, the Committee expresses concern regarding laws on such matters as lese majesty… and laws should not provide for more severe penalties solely on the basis of the identity of the person that may have been impugned."[193]

In February 2017, the UN Special Rapporteur on freedom of expression David Kaye stated that "*lesè majesté* provisions have no place in a democratic country" and that "the fact that some forms of expression are considered to be insulting to a public figure is not sufficient to justify restrictions or penalties" even if these figures include "those exercising the highest political authority".[194] Former Special Rapporteur Frank La Rue had previously clarified that the proportionality of *lesè majesté* provisions should be read in line with the international legal standards on defamation, and should not impose criminal penalties.[195]

Thailand

In Thailand, the criminal offence of *lesè majesté* has been extensively used to charge, convict and imprison individuals not only for expressing their opinions online, but also for merely 'sharing' or 'liking' posts on social media platforms relating to the King.[196] Article 112 of the **Criminal Code**

193 CCPR/C/GC/34, para 38.

194 OHCHR, 'Thailand: UN rights expert concerned by the continued use of lèse-majesté prosecutions', 7 February 2017, Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21149&LangID=E

195 Communication No. THA 5/2011 from UN Special Rapporteurs on freedom of expression and on the situation of human rights defenders to Government of Thailand, 10 June 2011, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=21153; Communication No. THA 10/2011 from UN Special Rapporteurs on freedom of expression, on the right to health and on torture and cruel, inhumane and degrading treatment to Government of Thailand, 6 January 2012, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=21524

196 iLaw Freedom of Expression Documentation Centre, '10 Q&A about *lèse majesté* law', Available at: https://freedom.ilaw.or.th/en/freedom-of-expression-101/QA-112; See for eg. January 2018 case of Chanoknan Ruamsap who was summoned to answer a *lèse majesté* charge for 'sharing' a BBC article on the King on Facebook, Thai Lawyers for Human Rights, 'Changes in Thailand's

('article 112') punishes "(w)hoever, defames, insults or threatens the King, the Queen, the Heir-apparent or the Regent" with three to fifteen years' imprisonment.[197]

Lesè majesté charges and convictions rose sharply after the military coup of May 2014, targeting individuals who made posts on social media platforms, particularly Facebook, which were deemed defamatory to the monarchy. At least 61 people were prosecuted in the year following the coup, and at least 33 people were charged between 2016 and 2017 during the period of mourning following the death of King Bhumipol.[198] As of May 2019, freedom of expression monitoring group iLaw documented that at least 99 individuals had been charged with *lesè majesté* offences, with some alleged offenders sent for interrogation or "attitude adjustment" sessions by the military.[199]

The military government also issued an order in 2014 extending the jurisdiction of military courts to include *lesè majesté* offences, in violation of international law.[200] In September 2016, Thailand's Prime Minister revoked orders which had granted military courts the jurisdiction to try *lesè majesté* cases.[201] However, charges relating to alleged violations committed before September 2016 continued to be tried before military courts until the Prime Minister issued another order ending the practice in July 2019.[202]

---

lèse majesté prosecutions in 2018', 15 January 2019, Available at: https://www.tlhr2014.com/?p=10431&lang=en

197 English translation of Thai Criminal Code B.E. 2499 (1956), Available at: http://library.siam-legal.com/thai-law/criminal-code-royal-family-sections-107-112/

198 Kas Chanwanpen, 'Junta reins in lese majeste', *The Nation,* 1 October 2018, http://www.nationmultimedia.com/detail/politics/30355507

199 iLaw, 'Latest statistics as of 21 May 2019', Available at: https://freedom.ilaw.or.th/en/content/latest-statistic

200 See for eg. ICJ on the case of Khathawut B., ICJ, 'Thailand: End prosecution of civilians in military tribunals', 19 November 2014, Available at: https://www.icj.org/thailand-end-prosecution-of-civilians-in-military-tribunals/; Principle 5 of the Draft Principles Governing the Administration of Justice through Military Tribunals clarifies that "military courts should, in principle, have no jurisdiction to try civilians", Available at: https://undocs.org/E/CN.4/2006/58

201 The Head of Thailand's National Council for Peace and Order (NCPO) and Thailand's Prime Minister, General Prayuth Chan-ocha, issued NCPO Order No. 55/2016 revoking NCPO Orders No. 37/2014, 38/2014 and 50/2014 which had allowed for the military court to have jurisdiction to try certain cases involving civilians, ICJ, 'Thailand: ICJ welcomes Order phasing out prosecution of civilians in military courts but government must do much more', 12 September 2016, Available at: https://www.icj.org/thailand-icj-welcomes-order-phasing-out-prosecution-of-civilians-in-military-courts-but-government-must-do-much-more/

202 The issuance by the Head of the NCPO (HNCPO) of HNCPO Order No. 9/2562 ended the trial of civilians in military courts. TLHR has, however, raised concerns about this order, See TLHR, 'Military authorities can still arbitrarily detain civilians Analysis of the Head of the NCPO Order no. 9/2562 that repealed some Announcements/Orders that are no longer necessary', 11 July 2019, Available at: https://www.tlhr2014.com/?p=12995&fbclid=IwAR3Aaizz-w5-0EWtPyd1FojKO0bDppesTkun_e3CHG9l8zrLTk5tmByp6ng&lang=en

Military courts have been shown to impose highly disproportionate punishments on individuals than civilian courts – including between 25 to 35 years' imprisonment terms (see cases below).[203] They also do not meet the requirements of the right to a fair trial by a competent, independent and impartial tribunal, guaranteed under article 14 of the ICCPR, which only allows for the use of military courts in a narrow range of circumstances. As the UN Human Rights Committee has noted, "the trial of civilians in military or special courts may raise serious problems as far as the equitable, impartial and independent administration of justice is concerned" and generally must be avoided.[204] In "exceptional" cases where they are used, they must be limited to "cases where the State party can show that resorting to such trials is necessary and justified by objective and serious reasons, and where with regard to the specific class of individuals and offences at issue the regular civilian courts are unable to undertake the trials."[205] In addition, trials must be "in full conformity with the requirements of article 14 and … its guarantees cannot be limited or modified because of the military or special character of the court concerned."[206]

In response to calls for the amendment or repeal of article 112, the Thai government has often responded to justify harsh penalties imposed under the law as necessary for "national security", "public order" and "social security", without clarifying how the law protects Thailand's territorial integrity.[207] ILaw – an independent free expression monitoring organization – has noted that "dubious and unclear over-interpretation" of the law has created a "climate of fear", self-censorship and even misuse of the law as

203 See OHCHR, 'Thailand: UN rights expert concerned by the continued use of lèse-majesté prosecutions', 7 February 2017 ('OHCHR, 7 February 2017'), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21149&LangID=E; OHCHR, 'Press briefing note on Thailand', 13 June 2017 ('OHCHR, 13 June 2017'), Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21734&LangID=E; Indeed, an elderly person sentenced to 20 years in prison for lèse-majesté died in prison in 2012. See Asian Correspondent, 'Thai grandfather sentenced to 20 years for lese majeste dies in jail', May 2012, Available at: https://asiancorrespondent.com/2012/05/thai-grandfather-sentenced-to-20-years-for-lese-majeste-dies-in-jail/

204 UN Human Rights Committee, General Comment No. 32, CCPR/C/GC/32, 23 August 2007, ('CCPR/C/GC/32'), para 22. Principles 2 and 5 of the UN Draft Principles Governing the Administration of Justice through Military Tribunals also clarifies that "military courts should, in principle, have no jurisdiction to try civilians", and that even where non-civilians are tried, "military tribunals must in all circumstances respect the principles of international law relating to a fair trial." See Commission on Human Rights, Report submitted by the Special Rapporteur of the Sub-Commission on the Promotion and Protection of Human Rights, Emmanuel Decaux, E/CN.4/2006/58, 13 January 2006.

205 CCPR/C/GC/32, para 22.

206 *Ibid.*

207 See Thailand's responses No. 52101/804, No. 52101/163, No. 52101/109 in 2014, 2016 and 2017 to Communications from Special Rapporteurs seeking clarification on lesè-majesté cases, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=32816; https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=32797; https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=33367

a tool of "revenge" in personal disputes.[208]

Most recently, the Thai government has begun to wield the **Computer-related Crimes Act** and a sedition-like offence under article 116 of the **Criminal Code** instead of article 112 to target alleged criticism of the monarchy online – a worrying development amidst Thailand's strengthening of measures to target "fake news" on social media platforms.[209] In October 2019, ***Karn Pongpraphapan***, a 25-year-old pro-democracy activist was arrested under the CCA for posting "inappropriate" online content against the monarchy on social media, even though the post had not explicitly referred to the Thai royal family (see below).[210] His post had been linked to an incident of a royal motorcade holding up traffic in Bangkok, soon after which a hashtag criticizing the motorcade had begun circulating widely on Twitter.[211] The day after his arrest, it was reported that the police had begun investigation into five other people linked to the allegedly offensive comments online.[212]

The arrest of Karn Pongpraphapan accentuates concerns that "criticism" or "offending the reputation of the monarchy" may be used as an arbitrary justification for State authorities to clamp down on expression and opinion online. His arrest came less than three months after Digital Economy and Society Minister Buddhipongse Punnakanta vowed to "purge" social media of insults against the monarchy, and before the opening of Thailand's Anti-Fake News Centre on 1 November, which civil society and academic observers have warned may be used to further surveil and censor speech online.[213] Thai authorities have also, in recent cases, required that

208 iLaw, '10 Q&A about *lèse majesté* law', Available at: https://freedom.ilaw.or.th/en/freedom-of-expression-101/QA-112

209 TLHR has noted this trend. In 2018, lawyer Prawet Prapanukul was convicted under article 116 of the Criminal Code after he had been indicted for ten Facebook message posts deemed in violation of article 112, and three other posts deemed in violation of article 116. In the same year, a visually impaired woman from Yala province, Nurahayadi Masao, who had been convicted for a Facebook post allegedly violating article 112, had her conviction overturned on appeal. Soon after, she was charged and convicted under the CCA for an audio clip she had 'shared' on Facebook in 2016. See TLHR, 'Changes in Thailand's *lèse majesté* prosecutions in 2018', 15 January 2019, Available at: https://www.tlhr2014.com/?p=10431&lang=en

210 Bangkok Post, 'Man arrested amid #royalmotorcade controversy', 8 October 2019 ('Bangkok Post, 8 October 2019'), Available at: https://www.bangkokpost.com/thailand/general/1767574/man-arrested-amid-royalmotorcade-controversy; Reuters, 'Thailand arrests man amid #royalmotorcade controversy', 8 October 2019 ('Reuters, 8 October 2019'), Available at: https://www.reuters.com/article/us-thailand-cyber/thailand-arrests-man-amid-royalmotorcade-controversy-idUSKBN1WN0GE.

211 The holding up of traffic – including an ambulance that had been made to wait in traffic – by the passing of a royal motorcade had resulted in rare expressions of overt criticism of the monarchy expressed online through the hashtag #royalmotorcade.

212 Teeranai Charuvastra, 'Gov't Says '5 More People' May Be Nabbed For Royal Insult', 8 October 2019, Available at: http://www.khaosodenglish.com/politics/2019/10/08/govt-says-5-more-people-may-be-nabbed-for-royal-insult/

213 Hathai Techakitteranun, 'Thailand to open anti-fake news centre by Nov 1 to address rumours on

persons arrested for violating *lesè majesté* provisions sign an agreement allowing the authorities to access information in their electronic devices without any court warrant, and committing that they will not make similar comments again, as a prerequisite to dropping criminal charges.[214]

As will be evident from cases below, *lesè majesté* has been used as a justification not only to prosecute statements critical of the monarchy but also to curtail academic or theoretical discussions about political theory, history, and governance. Expression or information deemed to offend the monarchy has not only been prosecuted pursuant to *lesè majesté* provisions in the law, but also other provisions relating to sedition or regulation of online communications.

Case of ***Karn Pongpraphapan***

In October 2019, **Karn Pongpraphapan**, a pro-democracy activist, was arrested and detained under the CCA following posts he had made on Facebook referring to how monarchic rule in Russia, France and Germany had been overthrown by popular revolution. His posts had come soon after widespread circulation of a hashtag on Twitter that expressed netizens' discontent with the manner in which a Thai royal motorcade had blocked traffic in Bangkok.

In announcing the arrest, the police implicitly alluded to a link between the activist's Facebook posts and the trending hashtag by stating that "(o)ver the last week, bad actors have started inappropriate hashtags on social media, resulting in the arrested person posting inappropriate content on Facebook which stirred hatred".[215]

Karn was released on bail, on conditions that he would not post similar content online again.[216]

social media platforms', *Straits Times,* 25 September 2019, Available at: https://www.straitstimes.com/asia/se-asia/thailand-to-open-fake-news-centre-by-nov-1-to-address-rumours-on-social-media-platforms; Zsombor Peter, 'Thailand's Anti-Fake News Center Fans Fears of Censorship', *VOA,* Available at: https://www.voanews.com/east-asia-pacific/thailands-anti-fake-news-center-fans-fears-censorship; See Section III (viii) for further discussion on the CCA.

214 ICJ communication with partners. In one instance, the ICJ was informed that such agreement had referred to the Cybersecurity Act to justify access to information in electronic equipment. See section III (viii) and footnote 531.

215 Reuters, 8 October 2019.

216 Bangkok Post, 8 October 2019.

Case of ***Vichai***

In June 2017, **Vichai**, a former insurance salesman, was sentenced to 35 years in jail under article 112 and the CCA – the longest sentence recorded for a lesè majesté offence – after he was found guilty of ten counts of posting information, including images and text, on Facebook deemed insulting to the monarchy.

Vichai was arrested in Chiang Mai province, but his sentence was handed down following a trial in camera at Bangkok Military Court.[217]

He was sentenced to 70 years in prison – seven years per count – a term that was commuted by half after he pleaded guilty at trial.

Case of ***Jatupat Boonpatararaksa (Pai Dao Din)***

In December 2016, Jatupat Boonpatararaksa, a student activist and human rights defender, known also as '**Pai Dao Din**' or 'Pai', was arrested and detained for 'sharing' a BBC Thai news article relating to the King on his Facebook page. He was thereafter moved from one police station to another for detention and interrogation on the basis that his case was "sensitive", "concerned national security, and it could pose a great threat to the public safety and order".[218]

In August 2017, Pai was convicted of violating article 112 of the Criminal Code and sentenced to five years' imprisonment, which was reduced to two and a half years following his guilty plea. Boonpatararaksa had been in pre-trial detention from 22 December 2016.[219]

In May 2019, Pai was released on royal pardon.[220]

217 Bangkok Post, 'Longest prison sentence ever for lese majeste', 9 June 2017, Available at: https://www.bangkokpost.com/thailand/general/1265778/longest-prison-sentence-ever-for-lese-majeste; OHCHR, 13 June 2017.

218 Communication No. THA 1/2017 from UN Special Rapporteurs on freedom of expression and on the situation of human rights defenders to Government of Thailand, 24 January 2017, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=22947; See also Human Rights Watch, ""To Speak Out is Dangerous" – The Criminalization of Peaceful Expression in Thailand', October 2019 ('HRW, October 2019'), p94, Available at: https://www.hrw.org/report/2019/10/24/speak-out-dangerous/criminalization-peaceful-expression-thailand

219 Communication No. THA 7/2017 from UN Special Rapporteurs on freedom of expression and on the situation of human rights defenders to Government of Thailand, 22 December 2017, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=23525

220 The Nation, 'Pai Dao Din released early on royal pardon', 10 May 2019, Available at: https://www.nationmultimedia.com/detail/breakingnews/30369158

Case of ***Thanakorn***

In December 2015, **Thanakorn**, a factory worker, was arrested at his house in Samut Prakan province for 'liking' a Facebook page that had allegedly contained lesè majesté content and for sharing content on Facebook that was deemed "sarcastic" and "defamatory" of the King's dog. This included clicking the 'like' button on a doctored image of the King.[221] He was held incommunicado in military custody soon after his arrest.[222]

Thanakorn was charged under article 112 of the Criminal Code and the CCA, and also article 116 of the Code for alleged sedition for posting an infographic on his account alleging corruption by high-ranking military officers with respect to the creation of Rajabhakti Park.[223] He faces up to 37 years' imprisonment in total under the charges.[224]

In November 2016, Samut Prakan Provincial Court ruled that his case was to be tried by the military court as it related to 'national security'. In June 2017, Thanakorn's final appeal for his case to be heard in a civilian court was rejected.[225] With the passage of the Prime Minister's order in 2019 to end trials of civilians by military courts, however, his case is likely to be transferred to a civilian court.

Thanakorn was released on bail after three months in detention, following multiple rejections of previous bail requests.[226]

221 Col. Burin Thongprapai, legal officer for the National Council for Peace and Order, noted "On December 2, he clicked 'Like' link on a doctored photo of the King and shared it with 608 friends". See Bangkok Post, 'Facebook user faces 32 years in prison for clicking 'Like'', 10 December 2015, Available at: https://www.bangkokpost.com/thailand/politics/790833/facebook-user-faces-32-years-in-prison-for-clicking-like

222 Human Rights Watch, 'Thailand: Junta Critic Feared 'Disappeared'', 11 December 2015, Available at: https://www.hrw.org/news/2015/12/11/thailand-junta-critic-feared-disappeared

223 [Thai] TLHR, 2016, Available at: https://tlhr2014.wordpress.com/2016/03/08/like112/

224 Prachatai English, 'Man accused of mocking late King's dog to be tried in military court', 30 November 2016, Available at: https://prachatai.com/english/node/6748

225 Prachatai English, 'Man charged for mocking late King's dog to face military court', 27 June 2017, Available at: https://prachatai.com/english/node/7240

226 PPT, Thanakorn Siripaiboon.

Cases of ***Thiansutham, Sasiwimol*** and ***Phongsak***

In March 2015, **Thiansutham**, a businessman, was sentenced to 25 years in jail under article 112 and the CCA for five posts made on Facebook deemed insulting to the monarchy. He was given a 10-year sentence per post, which was halved as he pleaded guilty at trial.

Thiansutham was arrested in December 2014 and held for questioning in an army base before charges were brought against him by the police.[227] His trial was held in camera before Bangkok Military Court.[228]

In August 2015, **Sasiwimol**, a hotel worker and mother of two, was sentenced to 56 years in jail under article 112 and the CCA for seven counts of Facebook posts deemed insulting to the monarchy. She received a term of eight years for each count, and had her sentence halved as she pleaded guilty at trial. Her trial was held in camera before Chiang Mai Military Court.[229]

In August 2015, **Phongsak Sribunpeng**, a tour operator, was sentenced to 30 years in jail under article 112 and the CCA for six posts made on his Facebook account which were deemed insulting to the monarchy. Phongsak received a 10-year imprisonment term for each of the six posts in question, resulting in a 60-year sentence. This sentence was halved as he pleaded guilty at trial. Phongsak's trial was heard in camera before a military tribunal.[230]

In 2017, the UN Working Group on Arbitrary Detention found the deprivation of liberty of Thiansutham, Sasiwimol and Phongsak had been "arbitrary" and had resulted in violations of their rights to free expression and fair trial.[231]

227 Bangkok Post, 'Military court jails man for 25 years over lese majeste', 1 April 2015, Available at: https://www.bangkokpost.com/thailand/general/514187/military-court-jails-man-for-25-years-over-lese-majeste

228 Bangkok Post, 'Facebook user gets 25 years in jail', 31 March 2015, Available at: https://www.bangkokpost.com/thailand/general/513735/facebook-user-gets-25-years-in-jail; OHCHR, 7 February 2017; BBC, 7 August 2015.

229 Political Prisoners in Thailand, 'Sasiwimol', Available at: https://thaipoliticalprisoners.wordpress.com/decidedcases/sasiwimol/; OHCHR, February 2017; BBC, 7 August 2015.

230 Political Prisoners in Thailand, 'Phongsak', Available at: https://thaipoliticalprisoners.wordpress.com/decidedcases/pongsak-s/; OHCHR, February 2017; BBC News, 'Thai courts give record jail terms for insulting king', 7 August 2015 ('BBC, 7 August 2015') Available at: https://www.bbc.com/news/world-asia-33819814

231 UN Working Group on Arbitrary Detention, 'Opinion No. 44/2016 concerning Pongsak Sriboonpeng (Thailand)', A/HRC/WGAD/2016/44, 17 January 2017, Available at: https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session77/A-HRC-WGAD-2016-44_en.pdf; UN Working Group on Arbitrary Detention, 'Opinion No. 51/2017 concerning Sasiphimon Patomwongfangam (Thailand)', A/HRC/WGAD/2017/51, 13 October 2017, Available at: https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_51.pdf; UN Working Group on Arbitrary Detention, 'Opinion No. 56/2017 concerning Thiansutham Suthijitseranee (Thailand)', A/HRC/WGAD/2017/56, 13 October 2017, Available at: https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session79/A_HRC_WGAD_2017_56.pdf.

Cambodia

In Cambodia, the criminal offence of *lesè majesté* was introduced into the Cambodian Criminal Code in the midst of a steep deterioration in human rights protection and rule of law leading up to the 2018 general elections.[232] In February 2018, following an exclusively internal and speedy review process, the Cambodian government introduced a new lesè majesté law, along with other constitutional amendments which imposed impermissible limitations on the rights to free association and freedom of assembly.[233]

Introduction of the lesè majesté provision under article 437 *bis* of the **Criminal Code** is one of a number of highly problematic legal measures brought into force by the ruling Cambodian People's Party to restrict fundamental freedoms surrounding the 2018 elections (which the party won by a landslide).[234] Article 437 *bis* criminalizes "insults to the King' with up to five years' imprisonment or a fine of up to ten million Riel (approx. USD 2,460) or both.[235] Legal entities found in violation of the law, including non-governmental and media organizations, can be subject to a ban on their activities, fines between ten million to 50 million Riel (approx. USD 2,460 to USD 12,300) and/or dissolution.[236]

232 ICJ, 'Misuse of law will do long-term damage to Cambodia' 26 July 2018, Available at: https://www.icj.org/misuse-of-law-will-do-long-term-damage-to-cambodia/; ICJ, 'Cambodia: deteriorating situation for human rights and rule of law (UN statement)', 27 June 2018, Available at: https://www.icj.org/hrc38-cambodia/; ICJ, 'Cambodia: weaponization of the law (UN Statement)', 22 March 2018, Available at: https://www.icj.org/hrc37cambodia/

233 ICJ, 'Submission of the International Commission of Jurists to the Universal Periodic Review of Cambodia', 12 July 2018, para 12, Available at: https://www.icj.org/wp-content/uploads/2018/07/Cambodia-UPR-Advocacy-Non-legal-submission-July-2018-ENG.pdf

234 ICJ, 'Cambodia: end efforts to introduce lèse-majesté law', 2 February 2018, Available at: https://www.icj.org/cambodia-end-efforts-to-introduce-lese-majeste-law/; Human Rights Watch, 'Cambodia: July 29 Elections Not Genuine', 25 July 2018, Available at: https://www.hrw.org/news/2018/07/25/cambodia-july-29-elections-not-genuine-0; Amnesty International, 'Cambodia: First 'royal insult' conviction a new low for government', 5 October 2018, Available at: https://www.amnesty.org/en/latest/news/2018/10/cambodia-first-royal-insult-conviction-a-new-low-for-government/

235 Leonie Kijewski, Soth Koemsoeun, 'National Assembly passes *lèse majesté* law, limits to freedom of association', *Phnom Penh Post*, 14 February 2018, https://www.phnompenhpost.com/national-politics/national-assembly-passes-lese-majeste-lawlimits-freedom-association

236 Ben Sokhean and Andrew Nachemson, 'As UN raises concerns over amendments, government says new *lèse majesté* law will apply to media', *Phnom Penh Post*, 22 February 2018, https://www.phnompenhpost.com/national/un-raises-concerns-over-amendments-governmentsays-new-lese-majeste-law-will-apply-media; Niem Chheng, Andrew Nachemson, 'Lèse-majesté law now in effect', *Phnom Penh Post*, 5 March 2018, https://www.phnompenhpost.com/national-politics/lese-majeste-law-now-effect

Case of ***Kheang Navy***

In May 2018, **Kheang Navy,** a 50-year-old primary school principal, was arrested and detained under article 437 *bis* of the Criminal Code for posting comments on Facebook which had allegedly insinuated a connection between the King and the dissolution of the main opposition political party, Cambodia National Rescue Party (CNRP) prior to the 2018 elections.[237]

Navy was questioned for hours without the presence of a lawyer – in violation of his right to have legal assistance – and held in pre-trial detention until he was convicted in October 2018 to two years in prison, with 18 months suspended.[238]

In November 2018, Navy was released.[239]

Case of ***Ban Samphy***

In May 2018, **Ban Samphy**, a 70-year-old former district leader of the opposition Cambodia National Rescue Party (CNRP) was arrested and charged under article 437 *bis* of the Criminal Code for sharing a post on Facebook that had allegedly criticized the King, which reportedly included a picture of Prime Minister Hun Sen and his wife and a picture of the King, along with a video clip of angry villagers who had been affected by flooding. His post had also compared the King with former kings of Cambodia.[240]

In October 2018, Samphy was convicted and sentenced to one year in prison, with five months suspended. In January 2019, however, an appeal court conducted a hearing in Samphy's absence – in violation of his fair trial right to be present at his trial – following an appeal by the deputy prosecutor to impose a lengthier sentence on Samphy. In February 2019, the court sentenced him to one year in prison, with two months suspended.[241]

In March 2019, Samphy was released.[242]

237 Kim Sarom, 'Lese majeste convict not free', *Phnom Penh Post,* 13 February 2019, Available at: https://www.phnompenhpost.com/national/lese-majeste-convict-not-free
238 Human Rights Watch, 'Political Prisoners Cambodia', October 2019, ('HRW Political Prisoners page 2019'), Available at: https://www.hrw.org/video-photos/interactive/2019/10/20/political-prisoners-cambodia
239 *Ibid.*
240 LICADHO, 'Cambodia's First *Lèse Majesté* Conviction', 5 October 2018, Available at: http://www.licadho-cambodia.org/flashnews.php?perm=261; HRW Political Prisoners page 2019.
241 HRW Political Prisoners page 2019.
242 *Ibid.*

Malaysia

In Malaysia, authorities have used sedition laws and laws regulating online communications to control perceived criticism of the monarchy on online platforms. As will be shown in sections III (iii) and III (iv) of this paper, these laws – namely the **Sedition Act 1948** and Section 233 of the **Communications and Multimedia Act 1998** ('CMA') – are in themselves not human rights compliant and have been misused to restrict freedom of expression and information in Malaysia.

The cases highlighted below reflect how, in the absence of lesè majesté laws, protection of the reputation of a person of royalty or institution of the monarchy can still be advanced as a justification by State authorities to limit free expression and information online. In April 2019, Malaysia's Home Minister stated that Malaysian police had investigated 97 cases of alleged insult against the monarchy on social media platforms between 2012 and March 2019, with 11 cases being charged in court under the Sedition Act or the CMA.[243] As will be seen below, use of the Sedition Act and the CMA in *Malaysia* is not dissimilar to the use of article 116 of the Criminal Code and the CCA in *Thailand* to curtail such expression online.

Section 3 of Malaysia's Sedition Act 1948 criminalizes any "act, speech, words, publication or other thing" having a "seditious tendency" to "bring into hatred or contempt or to excite disaffection against any Ruler or against any Government" – where 'Ruler' includes the *Yang di-Pertuan Agong* (the constitutional monarch of Malaysia) – or to "raise discontent or disaffection amongst the subjects of the *Yang di-Pertuan Agong* or of the Ruler of any State or amongst the inhabitants of Malaysia or of any State".[244] Section 4(1) punishes seditious offences with three years' imprisonment or a fine of up to RM 5,000 (approx. USD 1,207) or both for a first offence, and up to five years' imprisonment for a subsequent offence.[245]

243 Bernama, 'No need for lese-majeste laws in Malaysia, says Muhyiddin', *New Straits Times,* 1 April 2019, Available at: https://www.nst.com.my/news/nation/2019/04/475005/no-need-lese-majeste-laws-malaysia-says-muhyiddin

244 Sedition Act 1948 ('Sedition Act'), sections 3(1)(a), 3(1)(d), Available at: http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act%2015.pdf; There are nine royal families in Malaysia, the heads of whom are Sultans. Every five years, the Sultans elect one amongst themselves to be the *Yang di-Pertuan Agong*.

245 Sedition Act, section 4(1).

Cases of ***Eric Liew Chee Ling, Azham Akhtar Abdullah*** and ***Nur Alia Astaman***

In January 2019, **Eric Liew Chee Ling, Azham Akhtar Abdullah** and **Nur Alia Astaman** were arrested and investigated by the police pursuant to section 4(1) of the Sedition Act after posting comments on their social media accounts which were deemed insulting to Sultan Muhammad V after his abdication from his position as *Yang di-Pertuan Agong* a few days earlier.[246] These comments had made allegations regarding the Sultan's private life which had led to the abdication.

Liew's post had been made on Facebook and Abdullah and Astaman's comments were made on Twitter.[247] While Liew, Abdullah and Astaman removed their comments soon after their posting, screenshots of their posts were reportedly shared widely.[248]

Liew left his company soon after the incident, and Abdullah and Astaman were suspended from work and investigated by their companies regarding their online comments.[249]

246 Emmanuel Santa Maria Chin, 'Eric Liew, two others arrested for sedition over posts on former Agong', *Malay Mail*, 9 January 2019, Available at: https://www.malaymail.com/news/malaysia/2019/01/09/eric-liew-two-others-arrested-for-sedition-over-posts-on-former-agong/1710670; Agence France-Presse, 'Anger at arrests in Malaysia for alleged royal insults', *The Jakarta Post*, 10 January 2019, Available at: https://www.thejakartapost.com/seasia/2019/01/10/anger-at-arrests-in-malaysia-for-alleged-royal-insults.html

247 Channel News Asia, '3 arrested for insulting former Malaysian king on social media', 9 January 2019, Available at: https://www.channelnewsasia.com/news/asia/3-arrested-insult-sedition-malaysia-king-sultan-muhammad-v-11102288

248 Rachel Genevieve Chia, 'Angry netizens just got someone arrested and fired for 'insulting' Malaysia's former King – and two more people could face the same fate', *Business Insider Singapore,* 10 January 2019, Available at: https://www.businessinsider.sg/angry-netizens-just-got-someone-arrested-and-fired-for-insulting-malaysias-former-king-and-two-more-people-could-face-the-same-fate/

249 *Ibid.*

Case of ***Wan Ji Wan Hussin***

In September 2014, **Wan Ji Wan Hussin**, an Islamic preacher, was charged under section 4(1) of the Sedition Act for statements made on his Facebook account on religious matters and the Sultan of Selangor, Sultan Sharafuddin Idris Shah, where he had reportedly questioned the status of the Sultan as the head of Islam and claimed the Sultan's actions were not fully compliant with Islamic teaching.[250]

In April 2018, Wan Ji was sentenced to nine months in prison.[251] In July 2019, the Shah Alam High Court rejected his appeal against his sentence, instead increasing his imprisonment term to one year. The court, however, granted a stay against his sentence pending appeal.[252]

In a similar case:

In September 2014, activist **Ali Abd Jalil** was charged with three counts under the Sedition Act for Facebook posts allegedly insulting the Sultan of Selangor and the Johor royal family.[253] He was arrested, released, re-arrested and held in custody in different prisons before being released at the end of September.[254]

In October 2014, he fled to Sweden, fearing his personal safety, where he was granted political asylum in 2016.[255]

250 The Star Online, 'PAS ulama on sedition charge', 11 September 2014, Available at: https://www.thestar.com.my/news/nation/2014/09/11/pas-ulama-on-sedition-charge-the-expanel-member-accused-of-belittling-role-of-selangor-ruler/; Aysha A Zaharin, 'Sultanate affairs and free speech conundrum', *New Straits Times,* 31 July 2019, Available at: https://www.nst.com.my/opinion/columnists/2019/07/508834/sultanate-affairs-and-free-speech-conundrum

251 Rafidah Mat Ruzki, 'Penang CM's Office staff jailed for seditious statements against Selangor Sultan', *New Straits Times,* 9 April 2018, Available at: https://www.nst.com.my/news/crime-courts/2018/04/355163/penang-cms-office-staff-jailed-seditious-statements-against

252 Article 19, 'Malaysia: Court extends sentence for criticism of royalty', 9 July 2019, Available at: https://www.article19.org/resources/malaysia-court-extends-sentence-for-criticism-of-royalty/

253 Free Malaysia Today, 'Ali Abd Jalil says he's now a PR of Sweden', 19 July 2016 ('FMT, 19 July 2016') Available at: https://www.freemalaysiatoday.com/category/nation/2016/07/19/ali-abd-jalil-says-hes-now-a-pr-of-sweden/

254 Astro Awani, 'Ali Abd Jalil seeks political asylum in Sweden', 25 October 2014, Available at: http://english.astroawani.com/malaysia-news/ali-abd-jalil-seeks-political-asylum-sweden-46952

255 FMT, 19 July 2016; Adam Abu Bakar, 'Exiled activist in Sweden yearns for freedom in Malaysia', 2 September 2017, Available at: https://www.freemalaysiatoday.com/category/nation/2017/09/02/exiled-activist-in-sweden-yearns-for-freedom-in-malaysia/

Case of ***Fadiah Nadwa Fikri***

In July 2018, lawyer **Fadiah Nadwa Fikri** was investigated by the police under section 4(1) of the Sedition Act and section 233 of the CMA, for posting an article on the blog, 'Malaysia Muda', which had been critical of the interaction between Anwar Ibrahim, leader of the People's Justice Party (PKR), and Malaysian royalty.[256]

Soon after, in the same month, Fadiah was called in for questioning by the police under section 9(1) of the Peaceful Assembly Act for attending a solidarity event that had been held for her.[257]

In a similar case:

In August 2018, youth activist **Asheeq Ali Sethi Alivi** was investigated by the police under the Sedition Act and CMA for alleged insult of Sultan Muhammad V in a speech he made in a solidarity rally held to support Fadiah.[258]

iii. Laws on sedition

Sedition laws have often been used to restrict freedom of expression, due to overbroad provisions which allow for such abuse. This is evident from the cases described above in *Thailand* and *Malaysia* where sedition laws have been used to unduly limit speech relating to the monarchy. This section analyzes how sedition laws in not only *Thailand* and *Malaysia,* but also *Myanmar, Brunei* and *Philippines* have been misused to harass and penalize individuals expressing themselves on questions of public interest, by designating a wide range of expression as capable of causing "unrest" or "disaffection" or of compromising national security or public order.

256 The blogpost is accessible at: Fadiah Nadwa Fikri, 'Don't Kiss the Hand that Beats You', *Malaysia Muda,* 9 July 2018, Available at: https://malaysiamuda.wordpress.com/2018/07/09/dont-kiss-the-hand-that-beats-you/; See also FMT reporters, 'Drop all charges against lawyer Fadiah, says PJ MP Maria', *Free Malaysia Today,* 12 July 2018, Available at: https://www.freemalaysiatoday.com/category/nation/2018/07/12/drop-all-charges-against-lawyer-fadiah-says-pj-mp-maria/; FMT Reporters, 'Hakam condemns probe into lawyer Fadiah for sedition', *Free Malaysia Today,* 11 July 2018, Available at: https://www.freemalaysiatoday.com/category/nation/2018/07/11/hakam-condemns-probe-into-lawyer-fadiah-for-sedition/

257 Vinodh Pillai, 'At centre of sedition probe, Fadiah gets support from rights activists', *Free Malaysia Today,* 13 July 2018, Available at: https://www.freemalaysiatoday.com/category/nation/2018/07/13/at-centre-of-sedition-probe-fadiah-gets-support-from-rights-activists/

258 Nurul Azwa Aris, 'Cops seize activist's phone in probe over 'insulting' Agong', *Free Malaysia Today,* 14 August 2018, Available at: https://www.freemalaysiatoday.com/category/nation/2018/08/14/cops-seized-activists-phone-in-probe-over-insulting-agong/

Laws aiming to suppress "sedition" covered in this section are distinguishable from those in the proceeding section below which specifically address "national security" and maintenance of public order. Both types of laws, however, have been wielded in a very similar manner, focusing narrowly on suppressing expression or information deemed to pose a threat to the nation or the head of State as a representative of the nation. These laws, particularly sedition laws, have often been retained from the colonial era when they were used to suppress and silence local opposition to colonial rule.[259]

In *Thailand*, article 116 of the Criminal Code criminalizes as sedition any act to "raise unrest and disaffection amongst the people in a manner likely to cause disturbance in the country", while in *Myanmar*, section 124A of the Penal Code penalizes seditious acts which "bring into contempt or excite disaffection towards the Government".[260] These provisions can be employed to curtail any form of expression commenting on political issues or other questions of public importance.[261] Thus, in *Thailand*, a prominent leader of an opposition political party was charged with sedition soon after Thailand's 2019 national elections.[262] In *Myanmar*, high-profile critics of State Counsellor Aung San Suu Kyi have been charged under section 124A, at risk of a maximum term of life imprisonment.[263]

As noted in the section above on article 19(3), the UN Human Rights Committee has indicated that States must take "extreme care" to

259 See for eg. Commentary on the colonial-era sedition laws of British India. Mohan J. Dutta, 'Sedition laws, colonial legacy, and possibilities of dialogue', *Straits Times,* 20 February 2016, Available at: https://www.straitstimes.com/opinion/sedition-laws-colonial-legacy-and-possibilities-of-dialogue; Durba Ghosh, '100 Years Past Due: Why It's Time to Retire Colonial-Era Laws', *Huffington Post,* 5 May 2016, Available at: https://www.huffpost.com/entry/100-years-past-due-why-it_b_9853496?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAI-X0WnJ_CoPf0DNBXNrp1dMShbjaIfqL3yy7HpzzrylOb--yjwahURnDOlzTS97CjNpwWvOp5gtvoyN32fN-vOGoZV15FFo8CWWh_OPO7cete7nZDQ9rbFVG1wkyqZ0p54JqR8BLPP-MYwZSf8zcVjnBzGTivH4-4MXH2_j0bhY

260 Thai Criminal Code, article 116; Myanmar Penal Code, section 124A.

261 See iLaw, 'Section 116: When 'Sedition' is used as the obstruction of freedom of expression', 13 September 2017, Available at: https://freedom.ilaw.or.th/en/blog/section-116-when-%E2%80%98sedition%E2%80%99-used-obstruction-freedom-expression

262 Pravit Rojanaphruk, 'Thanathorn Likely To Face Military Court For Sedition', *Khaosod English,* 6 April 2019, Available at: http://www.khaosodenglish.com/news/2019/04/06/thanathorn-to-face-military-court-for-sedition/; John Reed, 'Thanathorn Juangroongruangkit charged with sedition', *Financial Times,* 6 April 2019, Available at: https://www.ft.com/content/77997228-583e-11e9-9dde-7aedca0a081a

263 In September 2018, Ngar Min Swe was given a seven-year imprisonment sentence and a fine of 100,000 kyat (approx. USD 70) for social media posts critical of Aung San Suu Kyi. See Human Rights Watch, 'Dashed Hopes: The Criminalization of Peaceful Expression in Myanmar', 31 January 2019, Available at: https://www.hrw.org/report/2019/01/31/dashed-hopes/criminalization-peaceful-expression-myanmar; In May 2019, ultra-nationalist monk Wirathu was charged with sedition for reportedly lewd remarks made during rallies against Aung San Suu Kyi. See Khin Moh Moh Lwin, 'Wirathu Faces Arrest After Being Charged Under Sedition Law, Say Police', *Myanmar Now,* 29 May 2019, Available at: https://www.myanmar-now.org/en/news/wirathu-faces-arrest-after-being-charged-under-sedition-law-say-police

draft sedition laws which are narrowly and strictly compliant with article 19(3) of the ICCPR and has clarified that "in circumstances of public debate concerning public figures in the political domain and public institutions, the value placed by the Covenant upon uninhibited expression is particularly high".[264] Cases above and below – in the contrary – show that political debate or commentary, reporting on government authorities and engagement in human rights advocacy, which should be protected speech are exactly the forms of expression which overbroad provisions in sedition laws have been used to curtail.

Malaysia

In Malaysia, the **Sedition Act 1948** has not only been applied to clamp down on online expression and information regarding royalty, as noted above, but also leaders of government. This was evident during the administration of former Prime Minister Najib Razak, whose government was voted out in Malaysia's 2018 general elections.[265] An advisor to Malaysian human rights lawyers' association, Lawyers for Liberty, noted that between 2013 and 2016, 170 cases had been brought under the Sedition Act, and that in 2015 alone, "during the peak of Najib's crackdown", 91 individuals were arrested, investigated or charged under the law.[266] Of these individuals, the ICJ documented that 36 academics, lawyers, politicians, students, and activists had been targeted under the law in the first three months of 2015.[267]

During the administration of the former Prime Minister, amendments were also made to the Sedition Act in 2015 to extend the offence of sedition to include the "publishing, distribution and importing of seditious publications", as well as "publication by electronic means" and acts which "cause to be published" seditious material and which "propagate" such material.[268] The 2015 amendments also extended powers of the court to include ordering individuals to remove online content deemed seditious, banning individuals from accessing an electronic device and ordering an officer "authorized under the Communications and Multimedia Act 1998" to restrict access

264 CCPR/C/GC/34, paras 30, 38.
265 Human Rights Watch, 'Malaysia: Drop Remaining Sedition Cases', 1 August 2018, Available at: https://www.hrw.org/news/2018/08/01/malaysia-drop-remaining-sedition-cases
266 Ida Lim, 'BN more restrained? Most sedition law abuses during your leadership, lawyer tells Najib', *Malay Mail,* 12 January 2019, Available at: https://www.malaymail.com/news/malaysia/2019/01/12/bn-more-restrained-most-sedition-law-abuses-during-your-leadership-lawyer-t/1711784
267 ICJ, 'Malaysia: stop amendments strengthening Sedition Act', 7 April 2015, Available at: https://www.icj.org/malaysia-stop-amendments-strengthening-sedition-act/
268 Sedition (Amendment) Act 2015 ('Sedition (Amendment) Act 2015'), sections 2, 4, Available at: http://www.federalgazette.agc.gov.my/outputaktap/20150604_A1485_BI_Act%20A1485.pdf

to online content deemed seditious.[269] The Malaysian Bar, the Advocates' Association of Sarawak and the Sabah Law Association criticized these penalties as being targeted specifically at expression online, particularly on social media platforms.[270] Penalties were also increased under the amended Sedition Act to a maximum sentence of seven years' imprisonment under section 3(1) – regardless of whether the offence was a first offence – and a maximum sentence of 20 years' imprisonment for a new "aggravated" offence of sedition causing "bodily harm" or "damage to property".[271]

In October 2018, the Pakatan Harapan coalition government announced a moratorium on the Sedition Act, which it soon after lifted, allowing the law to be used in circumstances involving "national security", public order and race and religious relations.[272] Prior to their election into power, Pakatan Harapan had committed to revocation of the Sedition Act in their Manifesto.[273] Despite this promise, in January 2019, four persons were arrested under the law, on the basis of preserving racial and religious harmony – which was criticized by the Malaysian Bar for being a disproportionate use of the law, when other domestic legal and non-legal measures could have been used in an appropriate manner to prevent potential societal conflict.[274] Similarly, in March 2019, seven organizers of a march commemorating International Women's Day were summoned by the police for questioning under the Sedition Act.[275]

269 Sedition (Amendment) Act 2015, sections 8, 10.

270 Malaysian Bar, the Advocates' Association of Sarawak and the Sabah Law Association, 'Joint Press Release | Amendments to the Sedition Act 1948 are Draconian, Militate Against the Freedom of Speech and Expression, and Interfere with the Independence of the Judiciary', Malaysian Bar Online, 17 April 2015, Available at: http://www.malaysianbar.org.my/press_statements/joint_press_release_%7C_amendments_to_the_sedition_act_1948_are_draconian_militate_against_the_freedom_of_speech_and_expression_and_interfere_with_the_independence_of_the_judiciary_.html; Boo Su-Lyn, 'Sedition Act revisions worst ever attack on free speech, lawyers say', *Malay Mail,* 8 April 2015, Available at: https://www.malaymail.com/news/malaysia/2015/04/08/sedition-act-revisions-worst-ever-attack-on-free-speech-lawyers-say/874199; The Star Online, 'Sedition Act amendments further limit media freedom, say journalists', 10 April 2015, Available at: https://www.thestar.com.my/news/nation/2015/04/10/sedition-act-amendments-further-restrict-media-freedom-say-journalists/

271 Sedition (Amendment) Act 2015, section 4.

272 Raynore Mering, 'Sedition Act: Malaysian Bar calls for return of moratorium, halt to investigations', *Malay Mail,* 11 January 2019, Available at: https://www.malaymail.com/news/malaysia/2019/01/11/sedition-act-malaysian-bar-calls-for-return-of-moratorium-halt-to-investiga/1711633; The Star Online, 'Gerakan urges govt not to enact a new Sedition Act', 13 May 2019, Available at: https://www.thestar.com.my/news/nation/2019/05/13/gerakan-urges-govt-not-to-enact-a-new-sedition-act/

273 See Manifesto at file:///C:/Users/User/Downloads/Manifesto_PH_EN.pdf

274 These four cases included the cases of Eric Liew Chee Ling, Azham Akhtar Abdullah and Nur Alia Astaman. See Raynore Mering, 'Sedition Act: Malaysian Bar calls for return of moratorium, halt to investigations', *Malay Mail,* 11 January 2019, Available at: https://www.malaymail.com/news/malaysia/2019/01/11/sedition-act-malaysian-bar-calls-for-return-of-moratorium-halt-to-investiga/1711633; Human Rights Watch, 'Malaysia: Keep Moratorium on Abusive Laws', 5 December 2018, Available at: https://www.hrw.org/news/2018/12/05/malaysia-keep-moratorium-abusive-laws

275 They were reportedly taken in for questioning for potential violations of section 4(1) of the

Case of ***Eric Paulsen***

In January 2015, **Eric Paulsen**, human rights lawyer and co-founder of Lawyers for Liberty, was arrested by approximately 20 police officers and detained under the Sedition Act for investigation, in relation to a post he had made on Twitter alleging that Malaysia's Islamic Development Department (Jakim) was promoting extremism.[276] Paulsen was charged under section 4(1)(c) of the Act in February.

In August 2018, the Attorney-General's Office withdrew the charge against Paulsen.[277]

Case of ***Zunar***

In April 2015, political cartoonist **Zunar** was charged with nine counts under the Sedition Act for posts he had made on his Twitter account criticizing a Federal Court decision following a trial of then-leader of a key opposition party, Anwar Ibrahim.[278] Zunar faced up to 43 years' imprisonment under section 4(1)(c) of the Sedition Act under the charges.

Between 2009 and 2015, Zunar, his sales assistants and the webmaster of his website and online bookstore had been arrested and detained for investigation under sedition charges in at least six separate occasions, for the publication and sale of his cartoon books.[279]

In July 2018, following a change in government after elections in which the Pakatan Harapan coalition which Anwar Ibrahim led was voted into power, the Attorney-General's Office withdrew its charges against Zunar.[280]

Sedition Act and section 9(5) of the Peaceful Assembly Act. ICJ, 'Malaysia: stop the harassment and intimidation of Women's March organizers', 15 March 2019, Available at: https://www.icj.org/malaysia-stop-the-harassment-and-intimidation-of-womens-march-organizers/

276 Frontline Defenders, 'Case History: Eric Paulsen', Available at: https://www.frontlinedefenders.org/en/case/case-history-eric-paulsen

277 Ida Lim, 'Prosecution drops sedition cases against PSM's Arul, lawyer Eric Paulsen', *Malay Mail,* 15 August 2018 ('Malay Mail, 15 August 2018'), Available at: https://www.malaymail.com/news/malaysia/2018/08/15/prosecution-drops-sedition-cases-against-psms-arul-lawyer-eric-paulsen/1662642

278 Astro Awani, 'Cartoonist Zunar claims trial to sedition charges', 3 April 2015, Available at: http://english.astroawani.com/malaysia-news/cartoonist-zunar-claims-trial-sedition-charges-57007

279 Communication No. MYS 1/2015 from UN Special Rapporteurs on freedom of expression, assembly and association and on the situation of human rights defenders to the Government of Malaysia, 25 February 2015, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=20953

280 Maizatul Nazlina, 'Zunar sedition case withdrawn', *The Star Online*, 31 July 2018, Available at: https://www.thestar.com.my/news/nation/2018/07/31/zunar-sedition-case-withdrawn-counsel-and-mp-also-freed-of-charges-under-act/

In a similar case:

In August 2018, following the change in government, the Attorney-General's Office also withdrew sedition charges against politician **S. Arutchelvan** which had been brought against him in November 2015, following his criticism of the Federal Court decision in Anwar Ibrahim's case.[281]

Brunei Darussalam

In Brunei, the **Sedition Act 1948** has been misused – along with other emergency laws and the **Internal Security Act 1982** – to maintain strict limitations on freedom of expression, assembly and association in the country, including on online expression.[282] Brunei is a country run by an absolute monarch since 1962, when Brunei declared a state of emergency and observed its last general elections. The Sedition Act's provisions banning "disaffection" against the Sultan are thus particularly pronounced as the Sultan holds absolute executive power in the nation.[283]

Section 3(1) of the Sedition Act criminalizes any "seditious intention" which "bring(s) into hatred or contempt or excite(s) disaffection against His Majesty the Sultan and *Yang Di-Pertuan* or the Government of Brunei", "raise(s) discontent or disaffection amongst the inhabitants of Brunei" or "promote(s) feelings of ill-will and hostility between different classes of the population of Brunei". Section 4 of the Sedition Act penalizes any act done with "seditious intention" with up to two years' imprisonment and a B$5,000 fine (approx. USD 3,697) for a first offence, and up to three years' imprisonment and a fine for subsequent offences.[284]

281 Malay Mail, 15 August 2018.

282 The Human Rights Foundation Center for Law and Democracy, The Brunei Project, 'Universal Periodic Review Submission for Brunei Darussalam: NGO Submission', 3 October 2018, Available at: https://s3-us-west-2.amazonaws.com/maven-user-documents/humanrightsfoundation/world/bw9J2ZPh20arNmRSWD2Ctw/0s96_E5ZLU2pNIW8tI7kdQ/Brunei_UPR_Submission_Final_(1).pdf?utm_source=HRF+Master+List&utm_campaign=fd851cbc1c-EMAIL_CAMPAIGN_2018_08_30_05_33_COPY_01&utm_medium=email&utm_term=0_2d05ae8b4f-fd851cbc1c-77959975

283 *Ibid*; The Commonwealth, 'Brunei Darussalam : Constitution and politics', Available at: http://thecommonwealth.org/our-member-countries/brunei-darussalam/constitution-politics

284 Sedition Act 1948 (1984 Ed.), Available at: http://www.agc.gov.bn/AGC%20Images/LOB/pdf/Cap.24.pdf

Case of ***Shahiransheriffuddin***

In July 2017, **Shahiransheriffuddin** bin Shahrani Muhammad, a government employee, was charged under section 4(1)(c) of the Sedition Act for an alleged seditious publication following a post he had made on his Facebook account questioning a Halal certification policy by the Ministry of Religious Affairs and its implications on small businesses in Brunei.[285]

Shahiran was thereafter reportedly taken by men to the Ministry of Religious Affairs for two days of investigation without access to legal counsel, before being charged under section 230 of Brunei's Syariah Penal Code with "insulting a member of the Muslim Council" and "questioning the rulings of the Muslim Council" – charges which remain unconfirmed as he was reportedly not provided with a copy of the charges against him despite requests for them.[286]

Shahiran faces up to two years' imprisonment and a B$5,000 fine under the Sedition Act, and up to 9 years' imprisonment and B$16,000 in fines under the Syariah charges.[287]

In October 2018, Shahiran fled to Canada, seeking asylum.[288]

Reported case of targeting on Whatsapp

In February 2019, an unnamed woman was detained and questioned by the Brunei police under section 4(1)(c) of the Sedition Act for several Whatsapp messages she had allegedly sent criticizing the police. A statement by the Brunei police provided no further information on her case, but reiterated the seriousness of an offence of making statements in violation of the sedition law.[289]

285 Fadley Faisal, 'Government employee charged with sedition', *Borneo Bulletin,* 28 July 2017, Available at: https://borneobulletin.com.bn/government-employee-charged-sedition/

286 The Brunei Project, Facebook post of 16 November 2018, Available at: https://es-la.facebook.com/thebruneiproject/posts/2023697287920428?__xts__%5B0%5D=68.ARAL4o3G9C3IF1wn-ocRZnCKAHi4zH71OrLVnCMXhxG3ZQAuko4z1-romQTvx13wp40CmH2TF_wZuOP8ABX7lw6yEgX-vtYERjBzkUcJUCiC0Lamt2pPtN3M3yy_1HBiUPvHUTFU17MEbCDL-bH7d4GpN1XvElRinPqD3JQV_zwr-P9OpjF1HyijIlE7Nci7xBn21aHj9Yr-B-9w8x-6ejJSMvMJvPQ4tkGFnkgw7PmHzLsPl1antrln5J48CpoC-2CkN-dLvXsClLM-xl_Wz0mQDwEWSLWqOC4BjCnoDBQF07w8YEyEdFKJMjW2Oo76UhXZ0qcGM-fHwiFp3laFO8LInAU8B&__tn__=-R; Matthew Woolfe, 'Brunei's Tightening Grip on Freedom of Expression', *New Naratif,* 7 June 2019 ('Woolfe, 7 June 2019') Available at: https://newnaratif.com/journalism/bruneis-tightening-grip-on-freedom-of-expression/share/xuna/4de7729ea5da-f28540ee79b3dca73d19/

287 *Ibid.*

288 CBC Radio, 'Gay asylum seeker in Vancouver fears he would be stoned to death in Brunei', 3 April 2019, [Transcript] Available at: https://www.cbc.ca/radio/asithappens/as-it-happens-wednesday-edition-1.5082934/gay-asylum-seeker-in-vancouver-fears-he-would-be-stoned-to-death-in-brunei-1.5082938

289 [Bahasa Melayu] Pasukan Polis Diraja Brunei, 'PPDB tegas terhadap maklumat tular', 27 Februari 2019, Available at: https://imgur.com/pMC4zlc; Woolfe, 7 June 2019.

Philippines

In the Philippines, the offence of sedition has been used to target members of the political opposition and critics of the ruling administration of President Rodrigo Duterte. This practice has been enabled through vague and overbroad legal provisions which allow for criminalization of a wide range of potential acts as "seditious".[290]

Under Title Three of Philippines' **Revised Penal Code** which covers "Crimes against Public Order", article 139 defines sedition as an offence "committed by persons who rise publicly and tumultuously in order to attain by force, intimidation, or by other means outside of legal methods", to "prevent the promulgation of any law", "prevent the government, or any public officer, from freely exercising its or his functions", "inflict any act of hate or revenge upon the person or property of any public officer", or "commit, for any political or social end, any act of hate or revenge against private persons or any social class". Article 140 penalizes an act of sedition with approximately six years' imprisonment and a fine of up to PHP 10,000 (approx. USD 195), while article 141 punishes "conspiracy to commit sedition" with between six months and six years' imprisonment and a fine of up to PHP 2,000 (approx. USD 39).[291]

Article 142 thereafter broadly defines the offence of "incitement to sedition" to include incitement "by means of speeches, proclamations, writings, emblems, cartoons, banners, or other representations" or through "publish(ing) or circulat(ing) scurrilous libels against the Republic of the Philippines" or which "tend to disturb or obstruct any lawful officer in executing the functions of his office", instigate individuals to "cabal and meet together for unlawful purposes", "disturb the peace of the community", "the safety and order of the Government" or "knowingly conceal such evil practices". Such offence is punishable with up to six years' imprisonment and a fine of up to PHP 2,000 (approx. USD 39).[292]

290 See ICJ, 'Righting Wrongs: Criminal Law Provisions in the Philippines related to National Security and their Impact on Human Rights Defenders', pp. 20 to 23, Available at: https://www.icj.org/wp-content/uploads/2015/03/Philippines-Criminal-Law-Provisions-Publications-Report-2015-ENG.pdf

291 Revised Penal Code, sections 139 to 141. Section 140 states that "The leader of a sedition shall suffer the penalty of prision mayor in its minimum period and a fine not exceeding 10,000 pesos. Other persons participating therein shall suffer the penalty of prision correccional in its maximum period and a fine not exceeding 5,000 pesos". Section 141 states that "Persons conspiring to commit the crime of sedition shall be punished by prision correccional in its medium period and a fine not exceeding 2,000 pesos". These sentences are subject to periods provided under section 27 of the Revised Penal Code. Philippines uses indeterminate sentencing, and judges have the discretion to impose sentencing based on the Indeterminate Sentence Law. Indeterminate Sentence Law, Act No. 4103, Available at: http://www.chanrobles.com/actno4103.htm

292 Revised Penal Code, section 142. Section 142 states that "The penalty of prision correccional in

Following the passage of the **Cybercrime Prevention Act**, offences committed under articles 139 to 142 on online platforms became subject to penalties "one degree higher than that provided for by the Revised Penal Code".[293] This is deeply problematic, as the CPA takes as its starting point the existing overbroad provisions in the Revised Penal Code and extends their reach to the online sphere, while increasing the penalties imposed on expression or information shared online. As noted above, articles 139 to 142 cover not only writings, acts or cartoons deemed "seditious", but also "other representations" which can affect nearly any medium of communication.

Legitimate advocacy regarding bills or laws or calls for legal reform could well fall under the broadly conceived "seditious" act of "preventing the promulgation of any law." Expression of criticism of government policy or the conduct of a State official could be prosecuted as conduct which will "prevent the government, or any public officer, from freely exercising its or his functions." Reporting of issues of public concern, such as corruption could be labelled as "seditious" and intended to "commit, for any political or social end, any act of hate or revenge against private persons or any social class". Similarly, prevention of the "cabal(ling) and meet(ing) together for unlawful purposes" could be invoked as a ground to justify the impairment of the right to the freedom of association and assembly of civil society or union groups who press the government on matters of public interest. "Disturbing the peace of the community" and "the safety and order of the Government" can cover nearly any form of civil action, human rights advocacy or calls for legal or administrative reform. Any of these activities conducted online may run afoul not only of the Revised Penal Code, but also the CPA, and incur more severe penalties in contravention of Philippines' international legal obligations.

Case of ***Vice President Maria Leonor ('Leni') Robredo and others***

In July 2019, the Philippine National Police's Criminal Investigation and Detection Group (CIDG) filed criminal complaints alleging incitement to sedition and other charges, including libel and cyber libel, against **Vice President Leni Robredo and 35 other individuals** who had

its maximum period and a fine not exceeding 2,000 pesos shall be imposed upon any person who, without taking any direct part in the crime of sedition, should incite others to the accomplishment of any of the acts which constitute sedition".

293 See Section V below, for further analysis of the CPA. Cybercrime Prevention Act of 2012, Republic Act No. 10175 ('CPA'), section 6, Available at: https://www.lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html; See above foonote 290 indicating Philippines uses indeterminate sentencing, where 'one degree higher' would enable the judge to impose penalties under a penalty term more severe than the one prescribed for under the Revised Penal Code.

increasingly expressed views critical of the administration of President Rodrigo Duterte.[294] Subject to section 142 of the Revised Penal Code and section 6 of the CPA, they face more than six years' imprisonment for alleged "incitement to sedition".

Among those targeted by the criminal complaints were four bishops, three priests, a former education secretary, senators, former senators, and senatorial candidates of the opposition Liberal Party, to which the Vice President also belongs, and officials of the Free Legal Assistance Group (FLAG) – which had provided legal assistance to victims' families in cases involving potentially unlawful killings perpetrated under the Duterte administration's "war on drugs".[295]

The criminal complaints were filed in relation to videos which had circulated on YouTube alleging links between the President and the drug trade in the Philippines. The complaints alleged the 36 individuals had "incited sedition" through alleged involvement in the creation and distribution of these videos.[296]

Notably, just before these complaints were filed, the UN Human Rights Council had, in July 2019, adopted a resolution expressing grave concern over the potentially unlawful killings and disappearances which had arisen from the Duterte administration's "war on drugs".[297]

In September 2019, prosecutors from the Department of Justice concluded a preliminary investigation into the case.[298]

294 Lian Buan, 'CIDG sues Robredo, LP, bishops for sedition over Bikoy videos', *Rappler*, 18 July 2019 ('*Rappler*, 18 July 2019'), Available at: https://www.rappler.com/nation/235729-cidg-sues-robredo-liberal-party-bishops-sedition-over-bikoy-videos; Human Rights Watch, 'Philippines: Drop Sedition Cases Against Duterte Critics', 23 July 2019, Available at: https://www.hrw.org/news/2019/07/23/philippines-drop-sedition-cases-against-duterte-critics

295 They included former education secretary Brother Armin Luistro; priests Father Flaviano Villanueva, Father Albert Alejo, Father Robert Reyes; Bishops Honesto Ongtioco, Teodoro Bacani Jr, Pablo Virgilio David, and Socrates Villegas; Senators Leila de Lima and Risa Hontiveros; former senators Antonio Trillanes IV and Bam Aquino; and Otso Diretso senatorial candidates Chel Diokno, Florin Hilbay, Gary Alejano, Romulo Macalintal, Samira Gutoc and Erin Tañada. In the Philippines, the President and Vice President are elected separately. See *Rappler*, 18 July 2019.

296 Raissa Robles, 'In Philippines, mysterious whistle-blower claiming Duterte's family took millions in drug kickbacks unveils his identity', *South China Morning Post,* 6 May 2019, Available at: https://www.scmp.com/news/asia/southeast-asia/article/3009090/mysterious-whistle-blower-videos-claiming-philippine; Jason Castaneda, 'Duterte goes for broke with opposition sedition charge', *Asia Times,* Available at: https://www.asiatimes.com/2019/07/article/duterte-goes-for-kill-with-opposition-sedition-charge/

297 See ICJ, 'The resolution on Philippines has been adopted – what now?', 19 July 2019, Available at: https://www.icj.org/the-resolution-on-philippines-has-been-adopted-what-now/; ICJ, 'ICJ joins call for UN investigation into Philippines 'war on drugs' killings', 19 June 2018, Available at: https://www.icj.org/icj-joins-call-for-un-investigation-into-philippines-war-on-drugs-killings/

298 Tetch Torres-Tupas, 'DOJ wraps up probe on sedition raps vs Robredo, 35 others', *Inquirer.net,* 12 September 2019, Available at: https://newsinfo.inquirer.net/1163946/doj-wraps-up-probe-on-sedition-raps-vs-robredo-35-others; See also Lian Buan, 'DOJ starts probe into Robredo, LP lawmakers in Bikoy complaint August 9', *Rappler,* 26 July 2019, Available at: https://www.rappler.com/nation/236211-doj-start-sending-subpoenas-robredo-lp-lawmakers-bikoy-complaint

iv. Laws which aim to protect the security of the nation or public order

While sedition laws aim to protect "public order" by preventing expression deemed insulting to or critical of the Head of State or members of a ruling government, other laws have been wielded to curtail free expression, which purport to ensure "public order" through protecting the State itself.

This section looks at how such laws in *Laos, Vietnam* and *Myanmar* allow for abusive interpretation and enforcement by officials who are given unfettered discretion to conflate the perceived interests of the ruling government with the security and order of the State itself. Such laws may be vaguely framed as laws to prevent "propaganda against the State", protect against the release of information deemed "prejudicial to the security of the State" or prevent "incitement" of crimes deemed to affect "public order". Public order and national security are two purposes recognized as legitimate for limitations on fundamental freedoms, including freedom of expression under article 19(3) of the ICCPR. However, any such limitations of restrictions must be strictly in line with the principles of legality, necessity and proportionality.[299]

In 2013, the Tshwane Principles were promulgated to provide guidance in the drafting, revision or implementation of laws with respect to the authority of the state to bar disclosure of information on national security grounds.[300] The Tshwane Principles provide guidance that information should be barred from disclosure only if disclosure poses a "real and identifiable risk of significant harm to a legitimate national security interest" (Principle 3); information should never be withheld "in any circumstances", if they concern "gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and systematic or widespread violations of the rights to personal liberty and security" (Principle 10A); no public entity may be exempt from disclosure requirements (Principle 5) and the State has a duty to publicly provide information on classification of information (Principles 11, 12).[301]

299 "The relation between right and restriction and between norm and exception must not be reversed." See CCPR/C/GC/34, para 21.

300 In 2013, the Tshwane Principles were released as the result of a process facilitated by the Open Society Justice Initiative and involving the participation of the ICJ and other civil society organizations, governments, former security officials, human rights defenders and academics. The Principles address in a detailed manner the standards to be applied when States seek to shield information from public disclosure. See ICJ, 'New global principles on the right to information launched', 12 June 2013, Available at: https://www.icj.org/new-global-principles-on-the-right-to-information-launched/

301 The Tshwane Principles available at: https://www.icj.org/wp-content/uploads/2013/06/Global-Principles-on-National-Security-and-the-Right-to-Information-Tshwane-Principles-June-2013.pdf

Lao People's Democratic Republic (Lao PDR)

In Laos, a one-party State where the regime has consistently imposed highly repressive restrictions on fundamental freedoms,[302] laws have consistently been employed to clamp down on these freedoms to protect "national interests", "traditional culture and dignity" and "social orderliness".[303]

The **Criminal Code** of Laos, under article 65, prohibits "propaganda against the Lao People's Democratic Republic" including "slandering the Lao People's Democratic Republic, or distorting the guidelines of the party and policies of the government, or circulating false rumors causing disorder" to the detriment of national security. This offence incurs a penalty of up to five years' imprisonment and a fine of between 500,000 to 10 million Kip (approx. USD 57 to USD 1,145).[304] Notably, article 23 of Laos' **Constitution** similarly prohibits all "cultural and mass media activities" contrary to "national interests" or "traditional culture and dignity."[305]

In October 2014, **Decree No. 327 On Information Management on the Internet** ('Decree No. 327') was enacted, imposing criminal sanctions on internet users for disseminating any information which "bribes or convinces the people of Laos, and abroad, to attack against the Lao People's Revolution Party, the government of the Lao PDR, or destroy the peace, independence, sovereignty, democracy, and prosperity of the Lao PDR" or "publicizes, distorts, and disseminates false propaganda in order to create discrimination against ethnic groups and against the nation".[306] Decree No. 327 further allows for the "monitoring, resisting and suppressing" of information on the internet "which threatens society, and stability of

302 In 2018, Freedom House gave Lao PDR a score of 12/100 for its protection of political rights and civil liberties – or lack thereof; In 2019, Reporters without Borders (RSF) ranked Lao PDR 171 out of 180 countries in its World Press Freedom Index. See Freedom House, 'Laos Profile', Available at: https://freedomhouse.org/report/freedom-world/2018/laos; RSF, 'Laos: No light at the end of the tunnel', Available at: https://rsf.org/en/laos

303 See for eg. ICJ, 'Lao PDR: the ICJ criticizes new Decree on Associations', 13 December 2017, Available at: https://www.icj.org/lao-pdr-the-icj-criticizes-new-decree-on-associations/; ICJ, 'Lao PDR – Southeast Asia Security Laws', Available at: https://www.icj.org/south-east-asia-security-laws/lao-pdr-southeast-asia-security-laws/; FIDH (International Federation for Human Rights) and the Lao Movement for Human Rights (LMHR), Briefing paper on Laos, 2 September 2016 ('FIDH, LMHR, 2 September 2016'), Available at: https://www.fidh.org/IMG/pdf/20160831_laos_foe_br_en.pdf

304 FIDH, Lao Movement for Human Rights, 'Joint UPR submission Lao People's Democratic Republic 35th session (January - February 2020)', 18 July 2019 ('FIDH, LMHR, 18 July 2019'), para 5, Available at: https://www.fidh.org/IMG/pdf/fidh-lmhr_lao_pdr_js_upr35_july_2018.pdf

305 FIDH, LMHR, 18 July 2019, para 5.

306 English translation of Decree On Information Management on the Internet No. 327/GOV ('Decree No. 327'), article 10, Available at: http://www.laoservicesportal.gov.la/index.php?r=site%2Fdisplaylegal&id=56#a10

the nation."[307] It also explicitly covers information shared on social media platforms, webpages and websites, extending criminalization of existing offences under Laos' Criminal Code to the online sphere in a manner to the operation of *Thailand*'s CCA, *Malaysia*'s CMA and *Philippines'* CPA have been as described above.

Case of ***Somphone Phimmasone, Lod Thammavong*** *and* ***Soukane Chaithad***

In March 2017, **Somphone Phimmasone, Lod Thammavong** and **Soukane Chaithad** were arrested upon returning to Laos from Thailand, where they had made posts on their Facebook accounts reportedly criticizing the Lao government of corruption and human rights violations.[308]

After being held incommunicado – in violation of articles 7 and 9 of the ICCPR – in May 2017, they appeared on State-run television at the police headquarters, where the news reported that they had been arrested for "threatening national security by using social media to tarnish the government's reputation".309

They were charged under articles 56 ("treason to the nation"), 65 ("propaganda against the Lao PDR") and 72 ("gatherings aimed at causing social disorder") under the Criminal Code.[310]

In a secret trial which reportedly took place in April 2017, Phimmasone was sentenced to 20 years' imprisonment and fined 210 million kip (approx. USD 24,100), Chaithad was sentenced to 16 years' imprisonment and fined 106 million kip (approx. USD 12,200), and Thammavong was sentenced to 12 years' imprisonment and fined 110 million kip (approx. USD 12,650).[311]

307 Decree No. 327, article 2.
308 FIDH, 'Three government critics jailed for up to 20 years', 16 May 2017, Available at: https://www.fidh.org/en/region/asia/laos/three-government-critics-jailed-for-up-to-20-years; Ron Corben, 'Rights Groups Call for International Community to Press Laos on Jailed Activists', *Voice of Asia*, 26 June 2017, Available at: https://www.voanews.com/east-asia/rights-groups-call-international-community-press-laos-jailed-activists
309 *Ibid.*
310 FIDH, LMHR, 18 July 2019, para 7.
311 Ounkeo Souksavanh, Richard Finney, 'Three Jailed Lao Workers Were Also Fined, Sources Say', *Radio Free Asia*, 29 June 2017, Available at: https://www.rfa.org/english/news/laos/fined-06292017173030.html; They remain in prison. See Ounkeo Souksavanh, Richard Finney, 'Lao Workers Jailed For Criticizing Government Are Separated in Prison', *Radio Free Asia*, 19 October 2018, Available at: https://www.rfa.org/english/news/laos/separated-10192018145914.html

Case of ***Houayheuang Xayabouly***

In September 2019, **Houayheuang Xayabouly** (also known as 'Mouay') was arrested under article 117 of the Criminal Code following a post she had made on Facebook of a live video in which she had been critical of the Lao government's response to severe floods in the southern provinces of Laos.[312]

She had reportedly said in the video:

"In this emergency situation, I am not in need of food and water yet, but yesterday a huge flood came and people here were up on the roofs of their houses trying to escape. Where is the helicopter for rescuing those people? … I cannot be silent as we have been in the past. The era of the regime keeping the eyes and mouths of the people closed has come to an end". [313]

After approximately five days in detention, following police investigation and interrogation and no reported assistance of a lawyer, she "confessed" to committing an illegal activity and for "having connections with 'bad elements' both in the country and abroad".[314]

In November 2019, Mouay was sentenced to five years in prison and fined 20 million Kip (approx. USD 2,280). She had been held in detention in Champasak provincial prison from the time of her arrest in September.[315]

Vietnam

In Vietnam, laws aiming to protect the reputation and security of the State have consistently been invoked to clamp down on freedom of expression and information online – particularly since 2016 when then-President Tran Dai Quang increased repression of expression perceived as

312 RFA Lao service, 'Lao Authorities Arrest Woman for Criticizing Flood Relief Efforts on Facebook', *Radio Free Asia*, 16 September 2019, Available at: https://www.rfa.org/english/news/laos/laos-houayheuang-xayabouly-09162019172839.html

313 *Ibid.*

314 RFA Lao service, 'Laos State Media: Woman Arrested for Criticizing Government on Facebook Confesses', *Radio Free Asia*, 17 September 2019, Available at: https://www.rfa.org/english/news/laos/laos-mouay-confession-bail-09172019164231.html

315 FIDH, 'Woman jailed for five years for criticizing the government online', 22 November 2019, Available at: https://www.fidh.org/en/region/asia/laos/woman-jailed-for-five-years-for-criticizing-the-government-online; As of 26 September 2019, her family and friends had not been allowed to visit Mouay in detention. RFA Lao service, 'Woman Held For 'Defaming' Laos is Refused Family Visits', *Radio Free Asia*, 26 September 2019, Available at: https://www.rfa.org/english/news/laos/refused-09262019131452.html

critical of the ruling Communist Party of Vietnam.[316]

There has been an increased crackdown on expression online, particularly by pro-democracy activists. In September 2019, Human Rights Watch noted that in the first nine months of 2019 alone, 11 individuals had been convicted and sentenced to prison for expression unwelcome by the government.[317] In May 2019, an Amnesty International report documented at least 128 "prisoners of conscience"[318] were being held in Vietnamese prisons. This number represented a spike from 97 such prisoners in 2018. Nearly 10 percent of detained persons had been prosecuted for comments made on social media platforms.[319]

Amnesty International's report highlighted that the implementation of amendments to the **Penal Code** in January 2018 had resulted in increased prosecutions of online expression under the law, while the coming into effect of Vietnam's **Cybersecurity Law** in January 2019 was likely to intensify surveillance and censorship of online expression.[320] Of the 128 documented cases, 45 individuals were imprisoned for "aiming to overthrow the State", more than 20 for "undermining national unity", more than 15 for "conducting propaganda against the State" or "making, storing or disseminating" such propaganda, more than 15 for "disturbing public order" or "disrupting national security" and more than 10 for "abusing democratic freedoms to infringe on the interests of the State". [321] An environmental activist was sentenced to life imprisonment for allegedly "aiming to overthrow the state".[322]

316 Human Rights Watch, 'World Report 2017: Vietnam – Events of 2016', Available at: https://www.hrw.org/world-report/2017/country-chapters/vietnam; Al Jazeera News, 'At least 128 prisoners of conscience in Vietnam: Amnesty', 14 May 2019, Available at: https://www.aljazeera.com/news/2019/05/128-prisoners-conscience-vietnam-amnesty-190513034714570.html; Mike Ives, 'Tran Dai Quang, Hard-Line Vietnamese President, Dies at 61', *New York Times,* 21 September 2018, Available at: https://www.nytimes.com/2018/09/21/obituaries/tran-dai-quang-dead.html

317 Human Rights Watch, 'Vietnam: New Arrest for Facebook Postings', 7 October 2019 ('HRW, 7 October 2019'), Available at: https://www.hrw.org/news/2019/10/07/vietnam-new-arrest-facebook-postings; As of September 2019, freedom of expression monitor, The 88 Project, noted that 266 individuals remained in detention for expression of peaceful dissent; ICJ communications with partners.

318 Amnesty International, 'Detention and Imprisonment', Available at: https://www.amnesty.org/en/what-we-do/detention/ . Amnesty International uses the characterization "prisoners of conscience" to refer to persons who have not used or advocated violence but is imprisoned because of who they are (based on sexual orientation, ethnic, national or social origin, language, birth, colour, sex or economic status) or what they believe (religious, political or other conscientiously held beliefs).

319 Amnesty International, 'Prisoners of Conscience in Viet Nam', 13 May 2019 ('Amnesty, 'Prisoners of Conscience in Vietnam'), Available at: https://www.amnesty.org/download/Documents/ASA4103032019ENGLISH.pdf

320 Amnesty International, 'Viet Nam: Surge in number of prisoners of conscience, new research shows', 13 May 2019, Available at: https://www.amnesty.org/en/latest/news/2019/05/viet-nam-surge-number-prisoners-conscience-new-research-shows/

321 Amnesty, 'Prisoners of Conscience in Vietnam', p 6.

322 Amnesty, 'Prisoners of Conscience in Vietnam', pp 20, 21.

These crimes are enshrined under Vietnam's **Penal Code of 1999**, and the amended Penal Code of 2015. Articles 79, 87, 88 and 89 of the 1999 Penal Code respectively criminalized the "carrying out (of) activities aimed at overthrowing the people's administration" with up to 20 years' imprisonment, life imprisonment or capital punishment; the "undermining of Vietnam's national unity policy" with up to 15 years' imprisonment; "conducting of propaganda" with up to 12 years' imprisonment; and "disruption of security" with up to 15 years' imprisonment.[323] Articles 245 and 258 respectively criminalized the "fomenting of public disorder" and "abusing democratic freedoms to infringe upon the interests of the State" with up to seven years' imprisonment.[324]

In 2018, the **Penal Code of 2015** came into effect, introducing article 109, which reduced penalties for "carrying out (of) activities aimed at overthrowing the people's administration" to 12 years' imprisonment; but retained under articles 116, 118 and 331, the 1999 Penal Code's hefty penalties for "sabotaging of national solidarity", "disruption of security" and "abusing of democratic freedoms to infringe upon the interests of the State".[325] Significantly, the 2015 Penal Code introduced article 117 criminalizing the "making, storing, distributing or disseminating of materials" that "oppose the State" with up to 20 years' imprisonment – which has been used to target the spread of information critical of the State online, particularly on Facebook.[326]

323 English translation of Vietnam Penal Code of 1999 (No. 15/1999/QH10), Available at: https://www.wipo.int/edocs/lexdocs/laws/en/vn/vn017en.pdf
324 *Ibid.*
325 English translation of Vietnam Penal Code of 2015 (No. 100/2015/QH13), Available at: https://www.wipo.int/edocs/lexdocs/laws/en/vn/vn086en.pdf; See also UN Recommendations on the 2015 Penal Code and Criminal Procedural Code of Viet Nam, 17 May 2017, Available at: file:///C:/Users/User/Downloads/UN%20Recommendations%20on%20PC%20and%20CPC%20of%20Vietnam%20-%2017%20May%202017.pdf
326 See for eg. Amnesty, 'Prisoners of Conscience in Vietnam', cases no. 20, 28, 72, 74, 79.

Case of ***Dao Quang Thuc***

In October 2017, **Dao Quang Thuc**, a retired primary school teacher, was arrested in Hòa Bình province under article 79 of the 1999 Penal Code for the alleged offence of "aiming to overthrow the State" after he had made posts and comments on social media platforms, including on Facebook, regarding corruption and environmental issues.[327] He was reportedly severely beaten and left without food following his arrest.[328]

In January 2019, Dao was convicted and sentenced to 13 years' imprisonment and five years of house arrest.[329] In June 2019, it was reported he had gone on hunger strike with four other political prisoners in protest against abusive conditions in their prison camp.[330]

Cases of ***Le Van Sinh, Nguyen Van Cong Em*** and ***Nguyen Quoc Duc Vuong***

(September 2019)

In September 2019, **Le Van Sinh**, a pro-democracy activist, was sentenced by the People's Court of Ninh Binh province to five years' imprisonment under article 331 of the 2015 Penal Code for allegedly "abusing democratic freedoms to infringe upon the interests of the State", for disseminating via Facebook 13 articles with content "distorting the policy of the state and party", alleged defamation of provincial officials and criticizing draft laws pertaining to cybersecurity and special economic zones in Vietnam.[331]

In September 2019, **Nguyen Van Cong Em**, a pro-democracy activist, was sentenced by the People's Court of Ben Tre province to five years' imprisonment and five years of probation under article 117 of the 2015 Penal Code for allegedly "making, storing or disseminating information

327 Amnesty, 'Prisoners of Conscience in Vietnam', case no. 11.
328 Richard Finney, An Nguyen, 'Retired Vietnamese Teacher Handed 14-Year Prison Term in Subversion Trial', *Radio Free Asia,* 19 September 2018, Available at: https://www.rfa.org/english/news/vietnam/subversion-09192018143141.html
329 Dao Quang Thuc was sentenced to 14 years' imprisonment and five years of house arrest at first instance, before the imprisonment term was reduced to 13 years by the judge who heard his appeal. See The 88 Project, 'Dao Quang Thuc', Available at: https://the88project.org/profile/7/dao-quang-thuc/
330 The 88 Project, 'Prisoners go on collective hunger strike to protest abusive conditions in prison camp No. 6 Nghe An', 27 June 2019, Available at: https://the88project.org/prisoners-go-on-collective-hunger-strike-to-protest-abusive-conditions-in-prison-camp-no-6-nghe-an/?fbclid=IwAR2e4T_CNeH1IbuVmIv8IZ1Erc6pji4IVs7QGtF8T77UpI0HFJnm99StL_8
331 The 88 Project, 'Criticizing Government Corruption on Facebook, Activist Le Van Sinh Sentenced to Five Years for "Abusing Democratic Freedoms"', 18 September 2019, Available at: https://the88project.org/criticizing-government-corruption-on-facebook-activist-le-van-sinh-sentenced-to-five-years-for-abusing-democratic-freedoms/

against the State", for using multiple Facebook accounts between October 2017 and February 2019 to make posts, share articles, and live-stream videos with content "distorting the policies of State and Party".[332]

Both Le Van Sinh and Nguyen Van Cong Em had been arrested in February 2019.

In September 2019, **Nguyen Quoc Duc Vuong**, a pro-democracy activist, was arrested and charged under article 117 of the 2015 Penal Code for allegedly "making, storing or disseminating information against the State", following written posts and live-stream videos he had posted on his Facebook account.[333]

Cases of ***Nguyen Van Phuoc*** and ***Pham Xuan Hao***

(October 2019)

In October 2019, **Nguyen Van Phuoc**, a pro-democracy activist, was sentenced by the People's Court of An Giang province to five years' imprisonment under article 117 of the 2015 Penal Code for allegedly "making, storing or disseminating information against the State", following posts he had made he had on his Facebook account.[334]

He was reportedly convicted for his activities on Facebook between 2016 and 2018, including live-streaming videos where he had criticized the Vietnamese government and sharing articles, images and video clips deemed insulting to the government and the Communist Party of Vietnam.[335]

In October 2019, **Pham Xuan Hao**, an architect and lecturer at the Faculty of Technology, Can Tho University, was sentenced to one year in prison for allegedly "abusing democratic rights and freedoms to infringe upon state interests" under article 331 of the 2015 Criminal Code.

In its judgment, the People's Court of Ninh Kieu District, Can Tho City,

332 The 88 Project, 'Second Activist Convicted in September for Facebook Postings: Nguyen Van Cong Em Sentenced to Five Years in Prison under Article 117', 20 September 2019, Available at: https://the88project.org/second-activist-convicted-in-september-for-facebook-postings-nguyen-van-cong-em-sentenced-to-five-years-in-prison-under-article-117/

333 HRW, 7 October 2019. It was unclear which exact posts he had made on Facebook formed the basis of his charges.

334 Defend the Defenders, 'Facebooker Nguyen Van Phuoc Convicted of "Conducting Anti-state Propaganda" with 5-year Imprisonment', 31 October 2019, Available at: http://www.vietnamhumanrightsdefenders.net/2019/10/31/facebooker-nguyen-van-phuoc-convicted-of-conducting-anti-state-propaganda-with-5-year-imprisonment/

335 ICJ communications with partners.

expressed its view that "(even) being an expert and having high social awareness", Pham had "still used Facebook to 'publish pessimistic information about Vietnam that negatively affects netizens and the public'".[336]

Cases of ***Nguyen Nang Tinh*** and ***Nguyen Ngoc Anh***

(November 2019)

In November 2019, **Nguyen Nang Tinh**, an activist and music teacher, was sentenced to 11 years in prison following a one-day trial by the People's Court of Nghe An province. He was arrested in May 2019 under article 117 of the 2015 Penal Code for reportedly "posting anti-state content online".[337]

The conviction was based on a series of posts he had made on Facebook. During his trial, Nguyen had stated that the account in question was not his, and that it had belonged to another person named 'Nguyen Nang Tinh'.[338]

In November 2019, **Nguyen Ngoc Anh**, a pro-democracy activist, was sentenced to six years in prison under article 117 of the 2015 Penal Code for allegedly "making, storing or disseminating information against the State", following posts he had made he had on his Facebook account.[339] While State media had characterized his posts as "reactionary" and intended to "badmouth" the State and incite protests, Nguyen's work had reportedly often covered issues of public interest and social concern such as reporting on a toxic waste spill, writing about electoral issues and about political prisoners.[340]

He was arrested in August 2018, before being sentenced in June 2019 to six years' imprisonment by a court in Ben Tre province following a summary trial. In November 2019, the National High Court at Ho Chi Minh City upheld the six-year sentence.[341]

336 The 88 Project, 'Can Tho: Former University Lecturer Jailed for Online Posting', 1 November 2019, Available at: https://the88project.org/former-university-lecturer-jailed-for-online-posting/

337 The 88 Project, 'Nguyen Nang Tinh', Available at: https://the88project.org/profile/376/nguyen-nang-tinh/

338 Bangkok Post, 'Vietnam jails music teacher for 11 years over 'anti-state' Facebook posts', 15 November 2019, Available at: https://www.bangkokpost.com/world/1795029/vietnam-jails-music-teacher-for-11-years-over-anti-state-facebook-posts

339 The 88 Project, 'Nguyen Ngoc Anh', 17 November 2019, Available at: https://the88project.org/profile/191/nguyen-ngoc-anh/

340 HRW, 'Vietnam: Free Activist Jailed for Facebook Posts', 5 November 2019, Available at: https://www.hrw.org/news/2019/11/05/vietnam-free-activist-jailed-facebook-posts

341 The term included five years on probation. See The 88 Project, 'Nguyen Ngoc Anh', 17 November

In similar cases:

From 26 November 2019, at least eight other individuals have been sentenced to prison for their activities online.[342]

Myanmar

In Myanmar, the **Official Secrets Act 1923** ('OSA') – which bans the "collection" or "communication" of information deemed "prejudicial to the safety or interests of the State' – has been used to penalize journalists who were performing their professional duties,[343] and there is a risk it could be used against others, including human rights defenders.

Section 3(1)(c) of the OSA penalizes the "obtaining, collection, recording, publishing or communication to any person of any …document or information… calculated to be, directly or indirectly, useful to an enemy" with up to 14 years' imprisonment where the information is deemed "in relation to the naval, military or air force affairs of the State of in relation to any secret official code".[344] Section 3(2) thereafter states that "it shall not be necessary to show that the accused person was guilty of any particular act" deemed prejudicial to the State and that "notwithstanding that no such act is proved against him, he may be convicted… if it appears his purpose was… prejudicial to the safety or interests of the State".[345]

Apart from overbroad provisions under the OSA which do not clarify who an "enemy" is and what "directly or indirectly being useful to an enemy" entails, the OSA lifts any burden of proof from the prosecution to substantiate a charge that a defendant has posed real risk of harm against the interests of the State. This fails to comply with international

2019, Available at: https://the88project.org/profile/191/nguyen-ngoc-anh/

342 Including Nguyen Chi Vung, Pham Van Diep, Vo Hoang Trung, Doan Viet Hoan, Ngo Xuan Thanh, Nguyen Dinh Khue, Huynh Thi To Nga and Huynh Minh Tam. ICJ communications with partners.

343 The OSA is one of a range of laws which have been misused to target journalists in Myanmar, including the abovenoted Telecommunications Law and Penal Code provisions which deliberately curtail freedom of expression, but also laws which do not pertain to freedom of expression at all, including, for example, the Unlawful Associations Act of 1908, the Aircraft Act of 1934 and the Import-Export Law of 2012. See Human Rights Watch, 'Dashed Hopes: The Criminalization of Peaceful Expression in Myanmar', 31 January 2019, Available at: https://www.hrw.org/report/2019/01/31/dashed-hopes/criminalization-peaceful-expression-myanmar; OHCHR, 'The Invisible Boundary – Criminal prosecutions of journalism in Myanmar: Report by the Office of the United Nations High Commissioner for Human Rights (OHCHR)', 11 September 2018, Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23531&LangID=E

344 English translation of Official Secrets Act 1923, Available at: http://freeexpressionmyanmar.org/wp-content/uploads/2017/07/Official-Secrets-Act-EN.pdf

345 *Ibid.*

standards, which require that public authorities adequately demonstrate the legitimacy of any restriction of information, that the process of classification of information be made public, and that information be restricted only "as long as necessary" to protect a legitimate security interest.[346]

Case of ***Wa Lone*** and ***Kyaw Soe Oo***

In December 2017, Reuters journalists **Wa Lone** and **Kyaw Soe Oo** were arrested in northern Yangon under section 3 of the ISA, following investigative work and reporting the journalists had engaged in to uncover human rights violations committed by the Myanmar military's security forces in Rakhine state.[347] Their report documenting the military's killing of ten Rohingya men in Inn Dinn village was published online on Reuters news website on 8 February 2018.[348]

Wa Lone and Kyaw Soe Oo were detained incommunicado for nearly two weeks before charges were brought against them.[349]

In April 2018, police officer Capt. Moe Yan Naing testified during pre-trial hearings that he had been instructed to 'frame' the journalists by planting on them documents related to security operations in Rakhine state.[350]

In July 2018, Yangon Northern District Court made a decision to extend the journalists' detention term, even as ICJ Legal Advisers monitoring the case noted that through six months of hearings, the prosecution had failed to provide credible evidence to substantiate a conviction.[351]

In September 2018, Wa Lone and Kyaw Soe Oo were convicted and sentenced to seven years' imprisonment.[352]

346 Tshwane Principles, Principles 4, 11, 16.
347 The Irrawaddy, 'Reuters Reports Arrested in Yangon Under Official Secrets Act', 13 December 2017, https://www.irrawaddy.com/news/burma/breaking-reuters-reporters-arrested-yangon-official-secrets-act.html; See ICJ, 'Reuters journalists detained in Myanmar: respect their rights, end their incommunicado detention', 18 December 2017, Available at: https://www.icj.org/reuters-journalists-detained-in-myanmar-respect-their-rights-end-their-incommunicado-detention/
348 Wa Lone, Kyaw Soe Oo, Simon Lewis, Antoni Slodkowski, 'Reuters Special Report: Massacre in Myanmar', Filed 8 February 2018, Available at: https://www.reuters.com/investigates/special-report/myanmar-rakhine-events/
349 ICJ, 'Myanmar: Reuters convictions a massive blow to the rule of law', 3 September 2018, Available at: https://www.icj.org/myanmar-reuters-convictions-a-massive-blow-to-the-rule-of-law/
350 Capt. Moe Yan Naing thereafter was sentenced to one year in prison under the Police Disciplinary Act and his family evicted from the police dormitory in which they had been living. See Eli Meixler, 'Myanmar Police Officer Who Said That Detained Reuters Reporters Were Set Up Has Been Jailed', *TIME*, 30 April 2018, Available at: https://time.com/5259232/myanmar-jail-police-whistleblower-reuters-reporters/
351 ICJ, 'Myanmar: officials must drop charges against Reuters journalists', 9 July 2018, Available at: https://www.icj.org/myanmar-officials-must-drop-charges-against-reuters-journalists/
352 Kyaw Phyo Tha, 'Calls Mount for Official Secrets Act to Be Amended in Wake of Reuters Case',

In May 2019, the journalists were released pursuant to a presidential amnesty.[353]

v. Laws which aim to protect the courts

Laws enacted or promulgated to protect certain aspects of the courts or judicial authority have also been wielded to curtail freedom of expression online. In *Singapore* and *Malaysia*, the instrument of "contempt of court" has been expanded to disproportionately extend powers of the court beyond a narrow legitimate aim of ensuring integrity and good order in court proceedings. In *Thailand,* contempt of court has been increasingly used in recent years to target independent individuals expressing disfavoured public comment.

As emphasized by the UN Human Rights Committee, where limitations to freedom of expression are adopted even for a legitimate purpose, such as to maintain public order, contempt of court proceedings and penalties imposed for exercising the right to free expression must be strictly necessary and proportionate to that end. This means they must be specifically "warranted in the exercise of a court's power to maintain orderly proceedings" and must not infringe upon the legitimate exercise of the rights of the defence.[354]

Where contempt proceedings are brought against lawyers, as in some cases highlighted below, they may serve to violate basic tenets governing the legal profession and protections to which lawyers are entitled and reflected in international standards. The UN Basic Principles on the Role of Lawyers makes clear that lawyers must "enjoy civil and penal immunity

10 September 2018, Available at: https://www.irrawaddy.com/news/burma/calls-mount-official-secrets-act-amended-wake-reuters-case.html; In a similar case, in July 2014, the Chief Executive Officer and four journalists with Unity Journal newspaper were sentenced to ten years in prison with hard labour for publishing a report alleging a Myanmar military facility had been used to manufacture chemical weapons. In April 2016, they were released pursuant to a presidential amnesty. See Zarni Mann, 'Unity Journalists Sentenced to 10 Years Imprisonment With Hard Labor', *The Irrawaddy*, 10 July 2014, Available at: https://www.irrawaddy.com/news/burma/unity-journalists-sentenced-10-years-imprisonment-hard-labor.html; PEN International 'Myanmar: Five journalists released following presidential pardon', 22 April 2016, Available at: https://pen-international.org/news/myanmar-five-journalists-released-following-presidential-pardon

353 BBC, 'Wa Lone and Kyaw Soe Oo: Reuters journalists freed in Myanmar', 7 May 2019, Available at: https://www.bbc.com/news/world-asia-48182712; In April 2019, the ICJ and 19 other organizations urged a parliamentary committee formed to review Myanmar's 2008 Constitution to amend the Constitution to guarantee the rights to free expression and information and media freedom in line with international human rights law. See ICJ, 'Joint statement: constitutional reform must guarantee the right to freedom of expression in Myanmar', 11 April 2019, Available at: https://www.icj.org/joint-statement-constitutional-reform-must-guarantee-the-right-to-freedom-of-expression-in-myanmar/

354 CCPR/C/GC/34, paras 24, 31.

for relevant statements made in good faith in written or oral pleadings or in their professional appearances before a court, tribunal or other legal or administrative authority" (Principle 20) and that they are, like other individuals, entitled to the rights to free expression and association and "have the right to take part in public discussion of matters concerning the law, the administration of justice and the promotion and protection of human rights" (Principle 23).[355]

Singapore

In Singapore, contempt of court proceedings have been used to curtail freedom of expression and information under the guise of 'maintaining orderly proceedings', particularly in cases of online criticism touching upon politically sensitive matters.

In October 2017, the **Administration of Justice (Protection) Act 2016** (AJPA) came into force in Singapore, despite well founded concerns raised by multiple organizations that its vague provisions could result in abusive interpretation and implementation, given existing trends of use of contempt of court under **common law** to limit freedom of expression.[356] Prior to the coming into force of the AJPA, contempt of court cases could be brought under common law by Singapore's High Court and Court of Appeal pursuant to section 7 of the Supreme Court of Judicature Act.[357]

The AJPA lowers the threshold for contempt in what is referred to as "scandalizing the Court", expanding judicial powers to punish such contempt with increased and onerous penalties. Section 3(1) criminalizes the "scandalizing of court" through (i) "impugning the integrity, propriety or impartiality" of judges by "intentionally publishing any matter or doing any act that… poses a *risk* that public confidence in the administration of justice would be undermined" (section 3(1)(a)); and (ii) "intentional" publishing of any material which interferes with pending court proceedings, or *sub judice*

355 UN Basic Principles on the Role of Lawyers 1990, Available at: https://www.ohchr.org/EN/ProfessionalInterest/Pages/RoleOfLawyers.aspx

356 FORUM Asia, Think Centre, 'Singapore: New Contempt of Court Law Further Curtails Limited Freedom of Expression', 20 August 2016, Available at: https://www.forum-asia.org/?p=21369; AWARE, 'AWARE statement on the Administration of Justice (Protection) Bill', 10 August 2016, Available at: https://www.aware.org.sg/2016/08/aware-statement-on-the-administration-of-justice-protection-bill/; Human Rights Watch, 'Singapore: Reject Overly Broad Contempt Law', 8 August 2016, Available at: https://www.hrw.org/news/2016/08/08/singapore-reject-overly-broad-contempt-law; Amnesty International, 'Singapore: Contempt of court bill is a threat to freedom of expression', 16 August 2016, Available at: https://www.amnesty.org/en/latest/news/2016/08/singapore-contempt-of-court-law/

357 This section is now repealed from the Supreme Court of Judicature Act (Chapter 322) Rev. Ed. 2007.

contempt (section 3(1)(b)).[358] Section 3(1)(a) reduced the threshold for "scandalizing" contempt to a mere "risk" of undermining public confidence in the judiciary, where the common law test established in the landmark case of *Attorney-General v Shadrake Alan* was to establish a "real risk" of such undermining of confidence .[359] This exacerbated a standard that was already deeply problematic. Meanwhile section 12(1) of the AJPA increased the maximum penalty for "scandalizing" contempt to three years' imprisonment or a fine of S$100,000 (approx. USD 72,051) or both, when under common law, a six-week imprisonment sentence and S$20,000 (approx. USD 14,410) fine had been deemed appropriate.[360]

Judicial proceedings are matters of critical public importance. The bringing into force of this law with its overbroad provision to criminalize any expression or information which can pose a "risk" to public confidence in the administration of justice will have a chilling effect on the capacity of lawyers, academics and the general public to comment on particular cases, or critically analyse questions of jurisprudence. This is particularly relevant in Singapore, where, even prior to the AJPA, contempt of court had been used to unnecessarily and unjustifiably curtail online expression. Following the passage into force of the AJPA, charges were brought against a human rights defender and opposition politician for comments made on Facebook, evidencing that risks that had been highlighted that the law would be used against expressions of public comment were not unfounded.

358 Administration of Justice (Protection) Act 2016 (No. 19 of 2016), Available at: https://sso.agc.gov.sg/Act/AJPA2016#legis

359 See *Attorney-General v Wham Kwok Han Jolovan and another matter* [2018] SGHC 222 at [39], referring to *Shadrake Alan v Attorney-General* [2011] 3 SLR 778 at [36], Available at: https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/os-510-2018-(ag-v-jolovan-wham)-(final)-pdf.pdf ('*AG v Wham Jolovan* [2018]')

360 Associate Professor David Tan, 'Any Risk Will Do – The New Law on Scandalising Contempt in Singapore', Singapore Law Gazette, September 2016, Available at: https://www.google.com/search?q=any+risk+will+do+new+law+on+scandalising+contempt+in+singapore&rlz=1C1CHBF_enTH830TH830&oq=any+risk+will+do+new+law+on+scandalising+contempt+in+singapore&aqs=chrome..69i57.8470j0j9&sourceid=chrome&ie=UTF-8; In analyzing cases relating to scandalizing contempt that had been brought before Singapore courts prior to the passage of the AJPA, Assoc. Prof. Tan from the National University of Singapore noted that courts had consistently acknowledged that contempt of court had to be balanced with the right to freedom of speech protected under article 14 of the Singapore Constitution, and highlighted tellingly that it was "ironic that the judiciary permits a wider latitude of criticism of itself than Parliament would otherwise tolerate (under the AJPA)".

Cases of ***Alex Au, Eugene Thuraisingam*** and ***Li Shengwu***

In March 2015, blogger **Alex Au Wai Pang** was fined S$8,000 (approx. USD 5,900) for contempt of court, following a post he made on his socio-political blog that raised questions about Singapore's courts' handling of petitions challenging section 377A of the Penal Code.[361] Au had previously written on section 377A, which criminalizes sex between men, and the rights of LGBTI individuals in Singapore.

In August 2017, lawyer **Eugene Thuraisingam** was fined S$6,000 (approx. USD 4,423) after he posted a poem about the death penalty in Singapore on Facebook in May 2017. He had reportedly posted the poem just before his client was hung for drug trafficking. The fine was imposed after Thuraisingam had deleted the post and posted a public apology after Singapore's Law Society notified him that his post could amount to contempt of court.[362]

In October 2017, committal papers were served on academic **Li Shengwu**, starting contempt of court proceedings for a Facebook post he made in July 2017, which alleged that *"the Singapore government is very litigious and has a pliant court system. This constrains what the international media can usually report."*[363] The post had been set on a "Friends Only" privacy setting.

361 Mong Palatino, 'Singapore Blogger Who Criticized Court Case of Anti-Gay Sex Law Fined for 'Scandalizing the Judiciary'', *Global Voices*, 8 March 2015, Available at: https://advox.globalvoices.org/2015/03/08/singapore-blogger-who-criticized-court-case-of-anti-gay-sex-law-fined-for-scandalizing-the-judiciary/; This case followed precedent set by the *Shadrake* case where journalist Alan Shadrake was sentenced to six weeks in prison and fined S$20,000 for contempt of court, following the release of his book on the criminal justice system in Singapore, as charges of criminal defamation were also brought against him.

362 Thuraisingam also faced disciplinary proceedings before the Council of the Law Society, following which he was fined S$5,000 (approx. USD 3,664). See Selina Lum, 'Lawyer Eugene Thuraisingam fined $6,000 for contempt of court over Facebook post on death penalty', *Straits Times*, 7 August 2017, Available at: https://www.straitstimes.com/singapore/courts-crime/lawyer-fined-6000-for-contempt-of-court-over-facebook-post-on-death-penalty

363 Selina Lum, 'Papers for contempt properly served on Li Shengwu in the US: Court of Appeal', *Straits Times*, 1 April 2019, Available at: https://www.straitstimes.com/singapore/papers-for-contempt-properly-served-on-li-shengwu-in-the-us-court-of-appeal

Cases of ***Jolovan Wham*** and ***John Tan***

In October 2018, civil rights activist **Jolovan Wham Kwok Han** and opposition politician **John Tan Liang Joo** were the first persons convicted under section 3(1)(a) of the AJPA.

Wham was convicted for a post he had made on his Facebook profile in April 2018, stating that *"Malaysia's judges are more independent than Singapore's for cases with political implications"*, following which the Attorney-General's Office began committal proceedings against him.

Tan was convicted following a post he made on his Facebook profile in May 2018, stating *"By charging Jolovan for scandalising the judiciary, the AGC only confirms what he said was true"*.[364]

In April 2019, both men were fined S$5,000 (approx. USD 3,685). Wham and Tan were further ordered to pay the Attorney-General's Chambers S$7,298 (approx. USD 5,378) and S$6,966 (approx. USD 5,133) respectively in legal costs and disbursements.[365]

Malaysia

In Malaysia, the contempt of court doctrine has been misapplied in a manner similar to Singapore to curtail comments made about the judiciary in public interest. Such misapplication has often targeted and controlled the free expression of lawyers, in their role as officers of the court, in contravention of the UN Basic Principles on the Role of Lawyers.[366]

Article 10 of Malaysia's **Federal Constitution** which guarantees the right to freedom of speech, assembly and association, allows Parliament to impose limitations to this right, under article 10(2)(a), "to provide against contempt of court".[367] Article 126, thereafter, confers upon the Federal Court,

364 *AG v Wham Jolovan* [2018], at [3] to [6].

365 Selina Lum, '$5,000 fine each for activist Jolovan Wham and SDP's John Tan for contempt of court', *Straits Times*, 29 April 2019, Available at: https://www.straitstimes.com/singapore/courts-crime/5000-fine-each-for-activist-jolovan-wham-and-sdps-john-tan-for-contempt-of; In 2008, Wham was sentenced to 15 days' imprisonment for contempt of court for wearing a T-shirt with a picture of a kangaroo dressed in judicial robes at the High Court. See Louisa Tang, 'Contempt of court: AGC seeks fine for activist Jolovan Wham, jail time for opposition party member', *Today*, 20 March 2019, Available at: https://www.todayonline.com/singapore/contempt-of-court-agc-seeks-fine-activist-jolovan-wham-jail-time-opposition-party-member

366 See A. Vijayalakshmi Venugopal, Kamal Halili Hassan, 'The Law of Contempt of Court in Malaysia: Considering Reforms' (2012) *Advances in Natural and Applied Sciences*, 6(8), pp. 1451-1464 ('Venugopal and Hassan, 2012') Available at: http://www.aensiweb.com/old/anas/2012/1451-1464.pdf

367 Federal Constitution of Malaysia, Available at: http://www.agc.gov.my/agcportal/uploads/files/

Court of Appeal and High Courts of Malaysia the power to punish contempt of court.[368] Other domestic laws extend this power to other subordinate courts, including Magistrates', Sessions and special courts.[369] There is, however, no statutory or authoritative legal definition otherwise in Malaysia.

Even as it operates as a **common law** doctrine, a clear definition of criminal contempt of court has not emerged within judicial pronouncements – allowing for wide judicial discretion that can limit freedom of expression.[370] Academic observers and practitioners have highlighted the need for reform to ensure not only clarity in definition, but also consistency in procedural rules and sentencing limits pertaining to criminal contempt cases – to prevent adjudication of such cases in an "arbitrary, subjective and personal" manner.[371] These commentators, along with the Malaysian Bar, have highlighted that criminal contempt of court should only be applied "sparingly", and as a "last resort in the interest of administration of justice", to limit infringement on the right to free expression.[372]

Case of ***Arun Kasi***

In February 2019, lawyer **Arunachalam s/o Kasi** ('Arun Kasi'), had committal proceedings initiated against him by Attorney-General Tommy Thomas, following his publication of two articles that month on online news portal, 'Aliran', where he had made comments said to be critical of the proceedings of the Federal Court of Malaysia.[373] His first article titled *'How a dissenting judgment sparked a major judicial crisis'*, and second article, titled *'Tommy Thomas must look into arbitration centre that sparked*

Publications/FC/Federal%20Consti%20(BI%20text).pdf

368 *Ibid.*

369 Venugopal and Hassan, 2012, pp. 1455 to 1456.

370 Venugopal and Hassan, 2012, pp. 1454 to 1455.

371 Venugopal and Hassan, 2012, p. 1463; Jerald Gomez, 'Contempt of Court — Freedom of Expression and the Rights of the Accused' (2002) 3 MLJ ccxli – ccciv ('Jerald Gomez, 2002'), Available at: http://jeraldgomez.com/wp-content/uploads/2018/01/MLJ-Contempt-of-Court-Freedom-of-Expression-and-the-Rights-of-the-Accused.pdf

372 In April 2019, the President of the Malaysian Bar noted, "To this end, the Malaysian Bar notes that the offence of "scandalising the Court" has been abolished in the United Kingdom (England and Wales). It bears reminding that the Court's power to punish for contempt should be used sparingly and, as recently held in our High Court, as a "last resort in the interest of administration of justice"." Abdul Fareed Abdul Gafoor, 'Press Release | Arun Kasi Found Guilty of Contempt of Court', 23 April 2019 ('Malaysian Bar, 23 April 2019'), Available at: http://www.malaysianbar.org.my/press_statements/press_release_%7C_arun_kasi_found_guilty_of_contempt_of_court.html; See also Venugopal and Hassan, 2012, p. 1463; Jerald Gomez, 2002, p. 20.

373 The Star Online, 'Contempt proceedings against lawyer Arun Kasi over Hamid affidavit articles in Aliran (updated)', 27 February 2019, Available at: https://www.thestar.com.my/news/nation/2019/02/27/contempt-proceedings-against-lawyer-arun-kasi-over-hamid-affidavit-articles-in-aliran#CA0XyKX8v4xL8PjE.99

judicial crisis', had intimated judicial misconduct and reportedly called for reform of Malaysia's Asian International Arbitration Centre.[374] Arun Kasi soon after challenged the committal proceedings on the basis that his statements amounted to fair criticism, and did not breach contempt.[375]

In April 2019, Arun Kasi was convicted and sentenced to 30 days in prison and a fine of 40,000 Ringgit (approx. USD 9,474), with 30 days' imprisonment in default of the fine.[376]

In a statement following the judgment, the Malaysian Bar expressed serious concern that the prosecution would "create a negative perception of a stifling effect on public discourse, which is exacerbated by the lack of clear parameters governing the offence", and reiterated the right of individuals to freely express fair comment on matters of public interest.[377]

Thailand

In Thailand, the contempt of court doctrine has been increasingly wielded against free expression. While the offence of contempt of court is situated within the Thai Civil Procedure Code, the doctrine has been expanded beyond its narrow definition to target even cases which do not directly concern court proceedings. Thus, in 2017, students who had taken a picture of themselves performing a "dabbing" dance move before Khon Kaen provincial court to express support for a student activist were charged with contempt, and an opposition politician was found guilty of contempt after broadcasting through Facebook Live on the premises of the Criminal Court (see below).[378]

374 *Ibid.*

375 The Star Online, 'Lawyer in AG contempt case: There's a difference between contempt and fair criticism', 28 February 2019, Available at: https://www.thestar.com.my/news/nation/2019/02/28/lawyer-in-ag-contempt-case-theres-a-difference-between-contempt-and-fair-criticism#oezVhdPHpktmjsdK.99

376 V Anbalagan, 'Lawyer Arun jailed 30 days, fined RM40,000 for contempt of court', *Free Malaysia Today,* 23 April 2019, Available at: https://www.msn.com/en-my/news/national/lawyer-arun-jailed-30-days-fined-rm40000-for-contempt-of-court/ar-BBWc5kD

377 Malaysian Bar, 23 April 2019.

378 Teeranai Charuvastra, 'Ever-Expanding Contempt Of Court Law Worries Lawyers', *Khaosod English,* 22 August 2017, Available at: http://www.khaosodenglish.com/news/crimecourtscalamity/courts/2017/08/22/contempt-court-worries-lawyers/; Four university students, Phayu Bunsophon, Chatmongkon Janchiewcharn, Narongrit Upachan and an unnamed law student, had staged the act of support before the court for activist Pai Dao Din. See Teeranai Charuvastra, 'Activists Calling For Pai Dao Din's Freedom Charged With Contempt Of Court', *Khaosod English,* 17 March 2017, Available at: http://www.khaosodenglish.com/politics/2017/03/17/activists-calling-pai-dao-dins-freedom-charged-contempt-court/; The opposition politician Watana Muangsook was a key Pheu Thai Party member and former commerce minister. See Bangkok Post, 'Facebook lands Watana in contempt', 22 August 2017, Available at: https://www.bangkokpost.com/thailand/politics/1310591/facebook-lands-watana-in-contempt

Sections 31 to 33 of the Thai **Civil Procedure Code** govern the offence of contempt of court, where section 32 provides that the "author, editor or publisher" of any "newspaper or printed matter" can be deemed to be in contempt of court if the publication, "during a trial of a case up to final judgement, contains or expresses in any way whatsoever any information or opinion intended to influence the public sentiment or the Court or any party or witness in the case, likely to prejudice the fair trial of such case", including "misrepresentation of case facts", "biased or inaccurate reporting", "unfair comment" or "inducement to commit perjury".[379]

This offence has been extended to apply to the Thai Constitutional Court by regulations promulgated by the court to clamp down on criticism of its operations or judgments. The Constitutional Court – tasked primarily with interpreting the Thai Constitution – has often been involved in adjudicating cases of political significance, and the independence of the court has often been questioned by observers in Thailand.[380] Notably, prior to Thailand's 2019 general elections, the court dissolved Thai Raksa Chart Party, a major opposition political party, weeks before the elections, and in May 2019, it suspended the Member-of-Parliament status of Thanathorn Juangroongruangkit, the leader of an opposition party that had gained prominence after coming in third in the elections.[381]

In March 2018, the **Organic Law on the Constitutional Court** came into force, granting the court the power to bring legal action against any comment on its ruling which is deemed "dishonest", "sarcastic", "rude" or "malicious" with penalties of up to one month in prison and/or a fine of up to THB 50,000 (approx. USD 1,652).[382] In October 2019, the 'Regulation

379 English translation of Thai Civil Procedure Code B.E. 2477, Available at: https://www.imolin.org/doc/amlid/Thailand_The%20Civil%20Procedure%20Code.pdf

380 Eugénie Mérieau, 'The Thai Constitutional Court, a Major Threat to Thai Democracy', *IACL-AIDC Blog*, 3 May 2019, Available at: https://blog-iacl-aidc.org/2019-posts/2019/5/3/the-thai-constitutional-court-a-major-threat-to-thai-democracynbsp; iLaw noted that among the incumbent judges of the Constitutional Court, two of the nine – including Nakharin Mektrairat and Punya Udchachon – had been recruited by the National Legislative Assembly, while five – Nurak Marpraneet, Chut Chonlavorn, Boonsong Kulbupar, Udomsak Nitimontree and Jaran Pukditanakul – whose terms were due to have expired in 2017, had their terms extended by Head of the NCPO Order No. 24/2017 issued by the NCPO. See iLaw, 'The 2019 Elections, of the NCPO, by the NCPO, and for the NCPO', Available at: https://ilaw.or.th/node/5004

381 Bangkok Post, 'Constitutional Court disbands Thai Raksa Chart', 7 March 2019, Available at: https://www.bangkokpost.com/thailand/politics/1640796/constitutional-court-disbands-thai-raksa-chart; Jitsiree Thongnoi, 'Thailand's constitutional court blocks Future Forward leader Thanathorn Juangroongruangkit's bid for prime minister role', *SCMP*, 23 May 2019, Available at: https://www.scmp.com/news/asia/southeast-asia/article/3011554/thailands-constitutional-court-blocks-upstart-politician; Notably, in 2007 and 2008, Thai Rak Thai and Palang Prachachon parties had similarly been dissolved. See Thitinan Pongsudhirak, 'TRC dissolution turns up political heat', 8 March 2019, Available at: https://www.bangkokpost.com/opinion/opinion/1640868/trc-dissolution-turns-up-political-heat

382 The law also states that the court can issue a warning, or order an offender to leave its premises.

of the Constitutional Court governing the Court's Procedures' entered into force, prohibiting "the distortion of facts or laws in the (Constitutional) Court's orders or judgments, or criticism of the Court's orders or judgments in bad faith, or using rude, sarcastic, provoking or threatening words" allowing for prosecution under section 39 of the Organic Law, at the risk of the above-noted penalties.[383]

Case of ***Watana Muangsook***

In August 2017, opposition politician and former commerce minister of Thailand, **Watana Muangsook** was given a suspended one-month prison sentence and fined THB 500 (approx. USD 16.50) for contempt of court for using Facebook's live video streaming app, 'Facebook Live', on court premises.[384] Watana was found to have violated sections 30 and 31 of the Civil Procedure Code. He was also ordered to remove the video clip from his Facebook account.[385]

In August 2017, Watana had broadcasted on Facebook Live at the Criminal Court, making comments on a case unrelated to the case he was there for, where he had expressed support for another opposition politician.[386] The contempt of court verdict was handed down amidst other cases under sedition and incitement laws and the CCA ongoing against him.[387]

Cases of ***Kovit Wongsurawat*** and ***Sarinee Achavanuntakul***

In August 2019, Associate Professor of political science **Kovit Wongsurawat** was summoned by the Constitutional Court to meet with its Secretary-General of Office for an alleged "inappropriate" post he had made on his Twitter account in June 2019.[388] In the Tweet, Kovit had criticized the Court for being *"beyond shameless"* with respect to a pending case before it where it had not suspended the Members-of-Parliament from their political duties, even as they were alleged to have stocks in media companies, while the court had previously revoked the MP status of

383 ICJ communications with partners.
384 Bangkok Post, 'Facebook lands Watana in contempt', 22 August 2017, Available at: https://www.bangkokpost.com/thailand/politics/1310591/facebook-lands-watana-in-contempt
385 *Ibid.*
386 Prachatai, 'Junta critic gets 1 year suspended jail term for contempt of court', 22 August 2017, Available at: https://prachatai.com/english/node/7337; iLaw, 'Case: Watana Muangsook', Available at: https://freedom.ilaw.or.th/en/case/801#progress_of_case
387 *Ibid.* See also HRW, October 2019, pp. 63 to 67.
388 Bangkok Post, 'Facebook lands Watana in contempt', 22 August 2017, Available at: https://www.bangkokpost.com/thailand/politics/1310591/facebook-lands-watana-in-contempt

Thanathorn Juangroongruangkit for that reason.[389]

In October 2019, it was reported that Assoc. Prof. Kovit had apologized to the court, and promised to clarify on Twitter that the cases were not similar. The court thereafter did not pursue the case.[390]

In August 2019, independent academic and political writer **Sarinee Achavanuntakul** was summoned by the Election Cases Division of the Supreme Court for referring to the abovementioned issue in an article she wrote titled '"*Danger of Overwhelming Legalism (once again): the case of media shareholding of lower house candidates'* that was published online on the Bangkok Business Newspaper's website in May 2019.[391]

In October 2019, the court dropped the case against her after she made an apology.[392]

***

In recent years, new laws have been enacted to regulate information online, control the spread of disinformation and hate speech online and ensure cybersecurity to combat contemporary threats faced by States and the individuals they are duty-bound to protect. These legislative efforts, however, do not generally appear to have been undertaken in good faith by governments in the region. The weaknesses of older laws have reappeared in more contemporary laws, and the patterns of abuse in their implementation have persisted.

Meanwhile a new generation of laws aiming to combat online disinformation and ensure cybersecurity have been introduced across the region. While it is too early to fully assess their implementation, the provisions on their face reflect serious shortcomings, which are not dissimilar to limitations that were evident in older laws covered in this paper. In effect, these more contemporary laws have expanded the scope in practice for abuse of the legal system to increase censorship of expression and information online.

***

389 *Ibid.*
390 Bangkok Business News, 'Kovit free from tweeting contempt of court post', 10 October 2019, Available at: https://www.bangkokbiznews.com/news/detail/850433
391 TLHR, 'The Election Cases Division of the Supreme Court Summons Ms. Sarinee for Contempt of Court', 6 September 2019, Available at: https://www.tlhr2014.com/?p=13620&lang=en; Bangkok Post, 'Courts act against media-shareholding critics', 29 August 2019, Available at: https://www.bangkokpost.com/thailand/politics/1739051/courts-act-against-media-shareholding-critics; The article in Thai is available at: https://www.bangkokbiznews.com/blog/detail/648489
392 ICJ communication with partners.

(b) Emerging legal frameworks

vi. Laws which aim to regulate information online

Laws enacted or promulgated to regulate information online towards the purported aims of protecting users of online networks and platforms and ensuring security of online platforms have been invoked to impermissibly restrict free expression and information. Laws in *Myanmar, Thailand, Indonesia, Malaysia, Philippines* and *Cambodia* have adopted similar frameworks to the laws previously covered in this paper – by targeting expression or information alleged to be defamatory, seditious, or detrimental to the security or interests of the nation. Laws and regulations controlling the dissemination of information online have been misused to target individuals, independent media outlets and journalists reporting on matters of public interest and concern.

As noted in Section III(a), *Myanmar's* Telecommunications Law was promulgated to "protect telecommunications service providers and users" and "supervise telecommunications service, network facilities and telecommunications equipment for national peace and tranquility and for public security"; *Thailand's* CCA regulates the online sphere to prevent "computer data… likely to cause damage to the protection of national security, public safety… or cause panic to the general public"; and *Indonesia's* UU ITE was brought into force to ensure the "use and utilization of Information Technology to maintain and strengthen the national union and unity in the national interest" and "prevent misuse with due regard to religious and social-cultural values of Indonesian society".[393] They have all been used to mount or support criminal defamation charges against individuals who merely exercised their fundamental freedoms online. Similarly, the CMA has been used in *Malaysia* along with sedition charges to curtail freedom of expression and information online.[394]

While these laws have already been discussed above to show how they have supplemented older laws in the region, this section now focuses on how key provisions have, in recent years, been crafted to directly address issues that have emerged in the digital age. Unfortunately, the patterns of abuse and their impacts are troublingly similar from a human rights perspective.

393 Telecommunications Law, sections 4(d), 4(e); CCA, section 14(2); UU ITE, introductory paras (d), (f).
394 See Sections III (ii), III (iii) above.

Malaysia

In Malaysia, the **Communications and Multimedia Act** – which was brought into force to "ensure information security and network reliability and integrity" and should "not be construed as permitting the censorship of the Internet" – has, in practice, been misused to permit online censorship through charging individuals and barring access to and blocking news websites who post information online deemed critical of the ruling regime.[395]

Sections 233 and 263(2) of the CMA, in particular, have been used to target free expression online.[396] In 2016, the Malaysian Bar Association warned that misuse of these sections would result in "a chilling effect on the freedom of opinion and thought and… a climate of fear that suffocates freedom of expression and threatens to silence Malaysians".[397] It noted that section 263(2) had been used to harass and intimidate independent media, and that in 2016 alone, at least 39 cases had been reported of individuals being questioned, arrested, charged or sentenced under the CMA.[398]

Section 233 of the CMA provides for criminal liability for any person who "by means of any network facilities or network service or applications service knowingly makes, creates, solicits, or initiates the transmission of any comment, request, suggestion or other communication" or "initiates a communication using any applications service… during which communication may or may not ensue" of any content which is "obscene, indecent or offensive" with "intent to annoy, abuse, threaten or harass another person". Violations may be punished with up to a year in prison or a fine of up to RM 50,000 (approx. USD 12,144) or both, and an increased fine of RM 1,000 (approx. USD 243) per day for a continuing offence. The same punishment is applicable for an offence under section 211, which prohibits "content applications service provider(s), or other person(s) using a content applications service" from

395 Communications and Multimedia Act 1998 ('CMA'), sections 3(2)(j), 3(3). Available at: https://www.unodc.org/res/cld/document/mys/communications_and_multimedia_act_html/Malaysia_Communications_and_Multimedia_Act_1998.pdf

396 See Article 19, 'Malaysia: The Communications and Multimedia Act 1998 – Legal Analysis February 2017' ('Article 19 CMA analysis'), Available at: https://www.article19.org/data/files/medialibrary/38689/Malaysia-analysis-Final-December.pdf

397 Malay Mail, 'Communications and Multimedia Act being abused like Sedition Act, says Malaysian Bar', 9 January 2017, Available at: https://www.malaymail.com/news/malaysia/2017/01/09/communications-and-multimedia-act-being-abused-like-sedition-act-says-malay/1288815

398 *Ibid.* In 2017, it was reported that the Malaysian Communications and Multimedia Commission (MCMC) – the country's regulatory body for the communications and multimedia industry – had investigated 146 cases in that one year under section 233, following which 56 investigation papers were initiated. It is unclear how many of these cases were politically motivated. See Bernama, 'Deputy minister: MCMC probed 269 cases under Communications and Multimedia Act', *Malay Mail,* 6 November 2017, Available at: https://www.malaymail.com/news/malaysia/2017/11/06/deputy-minister-mcmc-probed-269-cases-under-communications-and-multimedia-a/1503811

"providing content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person".[399]

Section 263(2) of the CMA, under the heading of "National Interest Matters", provides that "(every) licensee shall, upon written request by the (MCMC) or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence" under the domestic laws of Malaysia, "including, but not limited to, … preservation of national security".[400]

In September 2018, the Communications and Multimedia Minister announced that the government would look into amending provisions such as sections 211 and 233 to "ensure there is no political persecution (and) no abuse, to ensure that there is fairness and… ultimately… to regulate multimedia fairly".[401] In August 2019, however, the MCMC set up a WhatsApp hotline for members of the public to submit screenshots of social media posts deemed "inappropriate or negative" with respect to "race, religion and royalty" – raising concerns that even as this measure could be effective in the short run to prevent proliferation of hate speech online, it could result in policing of expression online by not only the government but also members of the general public.[402] The setting up of this hotline further raises concerns that the trend of increased surveillance and policing of cyberspace in Malaysia may continue to the detriment of free expression online.[403]

399 CMA, sections 211, 233.
400 CMA, section 263(2).
401 Bernama, 'Gobind: Communications and Multimedia Act to be amended', *The Star Online,* 4 September 2018, Available at: https://www.thestar.com.my/news/nation/2018/09/04/gobind-communications-and-multimedia-act-to-be-amended/
402 Shazwan Mustafa Kamal, 'Where is our democracy? MCMC complaint hotline means we still need policing, says Umno senator', *Malay Mail,* 18 August 2019, Available at: https://www.malaymail.com/news/malaysia/2019/08/18/where-is-our-democracy-mcmc-complaint-hotline-means-we-still-need-policing/1781742
403 The Malaysian Police have noted that the force 'constantly monitors' social media. See Malay Mail, 'Cops tracking down social media users who claimed to have witnessed Sungai Besi road rage incident', 13 August 2019, Available at: https://www.malaymail.com/news/malaysia/2019/08/13/cops-tracking-down-social-media-users-who-claimed-to-have-witnessed-sungai/1780335; Syed Jaymal Zahiid, 'IGP: Get rid of me and 126,000 cops will watch Twitter', *Malay Mail,* 25 March 2015, Available at: https://www.malaymail.com/news/malaysia/2015/03/25/igp-get-rid-of-me-and-126000-cops-will-watch-twitter/866283

Case of ***Khalid Mohd Ismath***

In October 2015, **Khalid Mohd Ismath**, a human rights defender and member of a political opposition party, was charged with 11 counts under section 233 of the CMA and three counts under the Sedition Act, for posting information on social media deemed "offensive" to the royal family of the state of Johor. One of his posts had reportedly criticized abuse of power by the Malaysian police in the state.[404]

Ismath was arrested and remanded, and his detention period extended under the Sedition Act. On 29 October, after 22 days in detention, he was released on bail.[405]

In a similar case:

In June 2016, **Muhammad Amirul Azwan Mohd Shakri**, a 19-year-old building site worker, was sentenced to one year in prison after pleading guilty to 14 charges under section 233 of the CMA for alleged insult of a member of the royal family of Johor. Shakri's sentence was thereafter commuted to two years in a reform school.[406]

Case of ***Fahmi Reza***

In February 2018, **Fahmi Reza**, a satirical artist and filmmaker, was sentenced to one month in prison and fined RM30,000 (approx. USD 7,281) after the Ipoh Sessions Court found him guilty of violating section 233 of the CMA for posting an allegedly "offensive" image on his Facebook account in February 2016. The image was of the artist's painting of then-Prime Minister Najib Razak as a clown, along with the logo of the MCMC.[407]

In November 2018, the Ipoh High Court commuted Reza's sentence to a fine of RM10,000 (approx. USD 2,427) and one month in prison in default. Reza thereafter submitted an appeal against his conviction.[408] In July 2019, Malaysia's Court of Appeal rejected Reza's appeal, and upheld

404 Frontline Defenders, 'Khalid Mohd Ismath', Available at: https://www.frontlinedefenders.org/en/case/case-history-khalid-mohd-ismath; See also Article 19 CMA analysis, p5.
405 *Ibid.*; The Malaysian Insider, 'Court allows activist Khalid interim bail but with conditions', HAKAM, 29 October 2015, Available at: https://hakam.org.my/wp/2015/10/29/court-allows-activist-khalid-interim-bail-but-with-conditions/
406 Article 19 CMA analysis, p5; Gabriel Samuels, 'Teenager jailed for insulting Malaysian royal family on Facebook', *The Independent,* 8 June 2016, Available at: https://www.independent.co.uk/news/world/asia/teenager-jailed-for-insulting-malaysian-royal-family-on-facebook-a7070436.html
407 Frontline Defenders, 'Fahmi Reza', Available at: https://www.frontlinedefenders.org/en/case/fahmi-reza-sentenced-prison-and-fined
408 *Ibid.*

his conviction.[409]

In a similar case:

In June 2016, a 76-year-old man was arrested and detained for three days after he posted a picture through a message on a WhatsApp group which was deemed insulting to then-Prime Minister Najib Razak.[410]

Cases of ***Sarawak Report, Medium*** **and** ***The Malaysian Insider***

In July 2015, the MCMC blocked '**Sarawak Report**', an independent news blog after it had reportedly released information evidencing a high-level corruption scandal involving then-Prime Minister Najib Razak and State-owned investment fund '1Malaysia Development Berhad' (1MDB), of which he was the sole shareholder and signatory. The 'Sarawak Report' publication alleged that the then-Prime Minister had misappropriated funds from 1MDB.[411]

The news blog was blocked on the basis that it had violated sections 211 and 233 of the CMA.

In August 2015, an arrest warrant was issued by the Malaysian authorities against the founder and editor of the 'Sarawak Report', **Clare Rewcastle Brown**, based on the accusations that she had violated the Penal Code for "activities detrimental to parliamentary democracy", "forging false documents" and obtaining material through "criminal leakages".[412] Soon after the 'Sarawak Report' was blocked, the MCMC publicly issued warnings that individuals spreading 'unverified news' on the 1MDB scandal could be found in violation of sections 211 and 233.[413]

In January 2016, the '**Medium**' blog was reportedly blocked by certain

409 *Ibid.*

410 The man, who went by the name of 'Pa Ya' on the messaging app, was released on bail after the police's request to extend his detention term was rejected by the Johor Bahru Magistrate's Court, in light of his old age and health problems. See Gabriel Samuels, 'Malaysian pensioner arrested for 'insulting prime minister Najib Razak on Whatsapp'', *The Independent,* 7 July 2016, Available at: https://www.independent.co.uk/news/world/asia/malaysia-prime-minister-whatsapp-photo-insult-pensioner-arrested-a7124476.html; Yee Xiang Yun, '76-year-old author who allegedly insulted Najib on WhatsApp released', *The Star Online,* 6 July 2016, Available at: https://www.thestar.com.my/news/nation/2016/07/06/author-who-allegedly-insulted-najib-released/

411 Communication No. MYS 3/2015 from UN Special Rapporteurs on freedom of expression and on freedom of assembly and association to the Government of Malaysia, 18 August 2015, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=20955

412 *Ibid.*

413 Hanis Zainal, 'Marina slams MCMC warning to social media users over 1MDB', *The Star Online,* 9 July 2015, Available at: https://www.thestar.com.my/news/nation/2015/07/09/marina-mcmc-social-media/

Malaysian internet service providers, including State-owned Telekom Malaysia. A week before, the MCMC had submitted a request to the blog to remove an article by 'Sarawak Report' on its page for alleged violation of section 233 of the CMA – which 'Medium' refused.[414]

In February 2016, the MCMC issued a decision to indefinitely block public access to independent news portal, '**The Malaysian Insider**' (TMI), for alleged violation of sections 233 and 263(2) of the CMA. The decision was linked to a TMI report that had reportedly quoted an anonymous source from the advisory panel of the Malaysian Anti-Corruption Commission (MACC), which had remarked on corruption claims relating to then-Prime Minister Najib Razak – contradicting official statements of the MACC.[415]

Philippines

In the Philippines, as earlier noted, penalties for offences relating to defamation or libel and sedition have been extended to the online sphere through the **Cybercrime Prevention Act** which was enacted to "protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts."[416]

Section 4 of the CPA lists, under "Punishable Acts", the offences of "illegal access", "illegal interception", "data and system interference", "misuse of devices", "cyber-squatting", "computer-related forgery, fraud and identity theft", "cybersex", and "child pornography". However, the criminal acts that fall under its purview extend far beyond these specific cyber-related crimes.[417] Sections 6 and 7 of the CPA dictate that "all crimes defined and

414 Medium Legal, 'The Post Stays Up', *Medium,* 27 January 2016, Available at: https://blog.medium.com/the-post-stays-up-d222e34cb7e7#.5v2jvdhuf; Judith Balea, 'Despite being blocked in Malaysia, Medium stands by Sarawak Report', *Tech in Asia,* 27 January 2016, Available at: https://www.techinasia.com/medium-stands-sarawak-report-blocked-malaysia

415 Steven Thiru, 'Misuse of the Communications and Multimedia Act must end', *Malaysia Kini*, 1 March 2016, Available at: https://www.malaysiakini.com/news/332239; Aizyl Azlee, 'Minister justifies TMI block, says due to contradictory report on MACC panel', *Malay Mail,* 26 February 2016, Available at: https://www.malaymail.com/news/malaysia/2016/02/26/minister-justifies-tmi-block-says-due-to-contradictory-report-on-macc-panel/1068543

416 CPA, section 2.

417 CPA, sections 4(a), (b), (c)(1), (c)(2). Notably, in 2014, the Supreme Court declared void and unconstitutional sections 4(c)(3) (which penalizes posting of unsolicited commercial communications), 12 (which authorizes the collection or recording of traffic data in real-time) and 19 (which authorizes the Department of Justice to restrict or block access to data). See ICJ, 'Supreme Court Decision re. Cybercrime Prevention Act of 2012', 21 February 2014, Available at:

penalized by the Revised Penal Code and special laws" are covered under the CPA where they are "committed by, through and with the use of information and communications technologies" and provide that the CPA will increase penalties "one degree higher than that provided for by the Revised Penal Code and special laws" where such crimes are committed online.[418]

The crime of "cyberlibel" covered under the CPA is a distinct example of how the law – implemented originally to "protect and safeguard the confidentiality, integrity, and availability of information and data" – goes beyond regulation of distinct cyber-related crimes, as covered under section 4. It specifically criminalizes defamation through section 4(c)(4) of the Act, which extends criminalization of the offence of libel "as defined in Article 355 of the Revised Penal Code" to acts "committed through a computer system or any other similar means which may be devised in the future." It also expands the possible penalties for such an offence.

In 2014, the Philippine Supreme Court upheld the constitutionality of section 4(c)(4) of the CPA. The ICJ and other organizations had publicly expressed the view that the provision would unlawfully restrict freedom of expression.[419] Furthermore, the ICJ noted that the CPA was not only incompatible with the Philippine Constitution, but also with Philippines' international obligations under the ICCPR, and that promulgation of the law raised risks of stifling freedom of expression.[420]

This law has since been construed widely by bodies charged with its implementation to target individuals expressing criticism against the ruling regime. In the case of *Vice President Leni Robredo and 35 other individuals*, the CPA allowed for politicians and lawyers to be targeted not only for alleged libel and "incitement to sedition" under the Revised Penal Code, but also the specific offence of "cyberlibel" and increased penalties for both types of crimes.[421] As will be seen below, the CPA has also been misused to curtail press freedoms in the country.

---

https://www.icj.org/se-asia-security-law/supreme-court-decision-re-cybercrime-prevention-act-of-2012/

418 CPA, sections 6, 7.

419 ICJ, 'Philippines: Supreme Court decision may stifle freedom of expression', 19 February 2014 ('ICJ, 19 February 2014') Available at: https://www.icj.org/philippines-supreme-court-decision-may-stifle-freedom-of-expression/; Noting also that organizations, including the National Union of Journalists of the Philippines, the Internet and Society Program of the UP College of Law, and the National Press Club, had filed petitions before the Supreme Court alleging section 4(c)(4) violated the right to free expression.

420 ICJ, 19 February 2014.

421 See Section III (iii).

Case of ***Rappler***

In February 2019, **Maria Ressa**, journalist and CEO and co-founder of independent news website, '**Rappler**', was arrested and detained by Philippines' National Bureau of Investigation (NBI) under charges of cyberlibel under section 4(c)(4) of the CPA. Ressa was released the following day after posting bail of PHP 100,000 (approx. USD 1,951).[422]

The charges related to a story Rappler had published in May 2012 about Filipino businessman Wilfredo Keng who, five years later, in October 2017 filed a complaint with the NBI against Ressa and other executives of Rappler, alleging that the article had maligned him by linking him with the illegal drug trade and human trafficking.[423]

Notably, the article was published before the CPA came into force. In February 2018, the NBI dismissed Keng's complaint on the basis that it had not met the one-year time limit prescribed for the filing of libel cases – as prescribed under the Revised Penal Code. In March 2018, however, the NBI revived Keng's complaint and filed it with the Department of Justice (DOJ).[424]

The DOJ thereafter mounted charges against Ressa and former Rappler journalist **Reynaldo Santos Jr.** – the author of the article – on the grounds that Rappler had made typographical edits to the original article in February 2014, constituting a 're-publication' which came after the enactment of the CPA and which could be seen as a "continuing crime until the libelous article is removed or taken down".[425] The DOJ further clarified that, despite a clear one-year limit prescribed under the Revised Penal Code, the prescriptive time-limit for filing of cyberlibel cases would instead be 12 years, in line with Republic Act No. 3326.[426]

422 Frontline Defenders, 'Maria Ressa Arrested on Charges of Cyber Libel, Released on Bail', Available at: https://www.frontlinedefenders.org/en/case/maria-ressa-arrested-charges-cyber-libel-released-bail
423 *Ibid.*
424 *Ibid.*
425 Tetch Torres-Tupas, 'NBI files cyber libel case vs Rappler', *Inquirer.net,* 8 March 2018, Available at: https://newsinfo.inquirer.net/973871/nbi-files-cyber-libel-case-vs-rappler-nbi-doj-cyber-libel-rappler
426 Lian Buan, 'DOJ: You can be sued for cyber libel within 12 years of publication', *Rappler,* 14 February 2019, Available at: https://www.rappler.com/nation/223517-doj-says-people-can-be-sued-cyber-libel-12-years-after-publication; Republic Act No. 3326, Available at: http://www.chanrobles.com/acts/actsno3326.html

In July 2019, the trial of Ressa and Santos began in Manila.[427]

This case is one of 11 legal actions faced in total by Rappler, Ressa, and Rappler's directors and employees. The news agency, which has been openly critical of the current government, has also been targeted for alleged tax evasion and alleged foreign control of a media company in violation of domestic law.[428]

Cambodia

In Cambodia, prior to the national elections of 2018, the government issued an **inter-ministerial order (*prakas*)** allowing the Ministries of Information, Interior and Post and Telecommunications to monitor, block and shut down websites, social media pages or other information circulated online that would "cause social chaos and threaten national security".[429]

This *prakas* was passed amidst a crackdown on independent media throughout the country leading up to the elections. This included the shutdown of more than 30 radio frequencies across the country, the release of the National Election Committee's 'Code of Conduct' for journalists which prevented them from reporting news "affecting political and social stability", the shutdown of a major independent newspaper – The Cambodia Daily – for alleged tax violations, and the sale of another key independent newspaper – Phnom Penh Post – to an investor with links to the Cambodian government, following which its editor-in-chief and some senior employees

427 Lian Buan, 'A look into a libel trial: First witnesses up in Maria Ressa case', *Rappler,* 23 July 2019, Available at: https://www.rappler.com/nation/236083-first-witnesses-maria-ressa-cyber-libel-case

428 See Lian Buan, 'Maria Ressa arraigned for cyber libel; SC may be next option', *Rappler,* 14 May 2019, Available at: https://www.rappler.com/nation/230577-maria-ressa-arraigned-cyber-libel-supreme-court-may-be-next-option-may-2019; Lian Buan, 'Court of Appeals denies Rappler appeal in SEC case', *Rappler,* 11 March 2019, Available at: https://www.rappler.com/nation/225347-court-appeals-denies-rappler-appeal-sec-case

429 Mech Dara, Hor Kimsay, 'Three ministries set up web-monitoring group to look out for 'fake news'', *Phnom Penh Post,* 7 June 2018, Available at: https://www.phnompenhpost.com/national/three-ministries-set-web-monitoring-group-look-out-fake-news; Cambodian Center for Human Rights, 'Cambodian groups seek revocation of new online directive ahead of elections', IFEX, 15 June 2018, Available at: https://ifex.org/cambodian-groups-seek-revocation-of-new-online-directive-ahead-of-elections/

were fired.[430] This crackdown has continued after the election.[431]

Case of shutdown of news websites prior to elections

In July 2018, the *prakas* appeared to have enabled the blocking of websites of key independent news outlets – including Voice of America, Radio Free Asia and Voice of Democracy – and websites of English newspapers two days prior to the general elections.[432]

The Director-General of Information and Broadcasting at the Ministry of Information noted that 17 websites had been targeted by his ministry, which in concert with the Ministries of Interior and Post and Telecommunications, sought to block the sites for 48 hours, on the basis that "contents of those new media (we)re provocative, very political in their tendencies, and … restricting to the election". Other sites supportive of the ruling Cambodian People's Party (CPP) government reportedly remained accessible.[433] CPP won the elections with approximately 80 percent of the vote.[434]

430 Niem Chheng, Ananth Baliga, 'Radio station booted off air', *Phnom Penh Post,* 24 August 2017, Available at: https://www.phnompenhpost.com/national/radio-station-booted-air; Mech Dara, Ananth Baliga, 'Government closes 15 radio stations', *Phnom Penh Post,* 25 August 2017, Available at: https://www.phnompenhpost.com/national/government-closes-15-radio-stations; Nareth Muong, Joshua Lipes, 'Cambodia to Monitor, 'Control' Online News Ahead of Upcoming Ballot', *Radio Free Asia,* 4 June 2018, Available at: https://www.rfa.org/english/news/cambodia/news-06042018162755.html; The Cambodia Daily, 'The Cambodia Daily to Close After 24 Years', Available at: https://www.cambodiadaily.com/cambodia-daily-close-24-years/; BBC, 'Phnom Penh Post: Firing and resignations after sale of Cambodian daily', 7 May 2018, Available at: https://www.bbc.com/news/world-asia-44027032

431 Notably, in July 2019, the Phnom Penh Municipal Court began the trial of two former Radio Free Asia journalists Uon Chhin and Yeang Sothearin for charges of espionage under section 445 of Cambodia's Criminal Code, for alleged "illegal collection of information for a foreign source", and further charges of alleged production of pornography. In May 2019, the UN Working Group on Arbitrary Detention found that the charges against both journalists had not been adequately substantiated and that the gravity of violation of their fair trial rights amounted to arbitrary deprivation of liberty. See UN Working Group on Arbitrary Detention, 'Opinion No. 3/2019 concerning Uon Chhin and Yeang Sothearin (Cambodia)' adopted by the Working Group on Arbitrary Detention at its eighty-fourth session, 24 April–3 May 2019, see paras 43, 51, 52, 59, 64, Available at: https://www.ohchr.org/Documents/Issues/Detention/Opinions/Session84/A_HRC_WGAD_2019_3.pdf; See also ICJ, 'Submission of the International Commission of Jurists to the Universal Periodic Review of Cambodia', 12 July 2018, para 26, Available at: https://www.icj.org/wp-content/uploads/2018/07/Cambodia-UPR-Advocacy-Non-legal-submission-July-2018-ENG.pdf; Human Rights Watch, 'Cambodia: Drop Case Against Journalists', 24 July 2019, Available at: https://www.hrw.org/news/2019/07/24/cambodia-drop-case-against-journalists

432 Prak Chan Thul, Amy Savitta Lefevre, 'Cambodia blocks some independent news media sites: rights group', *Reuters,* 28 July 2018, Available at: https://www.reuters.com/article/us-cambodia-election-censorship/cambodia-blocks-some-independent-news-media-sites-rights-group-idUSKBN1KH29Q

433 Erin Handley, 'Cambodia blocks 17 media websites before vote', Al Jazeera, 28 July 2018, Available at: https://www.aljazeera.com/news/2018/07/cambodia-blocks-17-media-websites-vote-180728103300267.html

434 Hannah Ellis-Petersen, 'Cambodia: Hun Sen re-elected in landslide victory after brutal crackdown', *The Guardian,* 29 July 2018, Available at: https://www.theguardian.com/world/2018/jul/29/cambodia-hun-sen-re-elected-in-landslide-victory-after-brutal-crackdown

vii. Laws which aim to control spread of "disinformation" online

In recent times, laws have come into force to regulate online information in order to address the spreading of "disinformation" or "false information" online. This section highlights laws in Thailand, Indonesia, Malaysia, Brunei, Singapore, Philippines and Laos. It notes that in practice, justifications for criminalizing the "new" offence of spreading disinformation often overlap with "old" broad-brush arguments to protect "security", "public order" and "stability" which have fueled misuse of earlier laws.

Most existing laws governing electronic information or telecommunications include the offence of intentionally spreading "false or misleading data" online. Sections 14(1) and (2) of *Thailand's* CCA penalize the "entering of false computer data into a computer system… likely to cause damage to the general public" or "to the protection of national security, public safety, or panic to the general public." Article 28(1) of *Indonesia's* UU ITE imposes penalties on any person who "knowingly and without authority disseminates false and misleading information resulting in consumer loss in electronic transactions". Sections 211(1) and 233(1)(a) of *Malaysia's* MCA ban the provision of "false content" along with "obscene or offensive" content "with intent to annoy, abuse, threaten or harass any person." Section 29 of *Brunei's* Telecommunications Act penalizes any person who "transmits or causes to be transmitted by telecommunication a message which he knows to be false or fabricated".[435]

More recently, some countries have brought into force specific laws to govern spreading "false information". These laws already appear to be at high risk of abuse because they include the same severe limitations that have plagued older laws in the region. This section begins with the positive example of *Malaysia*, where an 'anti-fake news' law brought into force before its 2018 elections was recently repealed by its new government.

Malaysia

In April 2018, a month before the general elections, **Malaysia's Anti-Fake News Act (AFNA)** came into force, amidst significant criticism that the law would be misused to curtail freedom of expression, opinion and

435 The penalty for such an offence is five years' imprisonment and a fine of B$24,000 (approx. USD 17,770). Telecommunications Act 1974 (Cap. 54), Available at: http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Chp.54.pdf

information online.[436] In October 2019, however, following the election of the new Pakatan Harapan coalition government, a bill to repeal the AFNA was passed through the lower house of the Parliament, which looks set to take effect within a year.[437] Although it is a commendable development that the law will now not be enacted, the AFNA is another example of a law that would have rolled back rights protections online, if it had been rushed into force before the elections.

Overbroad provisions under sections 4, 5 and 10 of the AFNA allowed for government authorities not only to hold criminally liable any person who "creates, offers, publishes, prints, distributes, circulates or disseminates any fake news or publication containing fake news", but also any person who "abets" or "directly or indirectly" provides "financial assistance" to the offence.[438] Severe penalties of up to six years' imprisonment, fines of up to RM 500,000 (approx. USD 121,212) or RM 3,000 (approx. USD 727) for every day of a continuing offence, were prescribed. Section 6 of the AFNA thereafter obliged any person "having in his possession, custody or control any publication containing fake news to immediately remove such publication" at risk of fines of up to RM 100,000 (approx. USD 24,252) or up to RM 3,000 (approx. USD 727) per day for every day of a continuing offence.[439] Sections 4 and 6 potentially incentivized online intermediaries, such as social media platforms, administrators of web or media pages and search engines, to remove content "immediately" at risk of hefty criminal sanctions, without adequate consideration to transparency, due process of law or rights protection.[440]

Extra-territorial application permitted under section 3 of the Act to control any "fake news" affecting Malaysia or "any person affected by the commission of an offence who is a Malaysian citizen" also violated the right

436 ICJ, 'Malaysia: Anti-Fake News Bill threatens freedom of expression, may lead to the suppression of critical speech', 27 March 2018, Available at: https://www.icj.org/malaysia-anti-fake-news-bill-threatens-freedom-of-expression-may-lead-to-the-suppression-of-critical-speech/; Southeast Asian Press Alliance, 'Infographic: Malaysia's Anti-Fake News Bill', 3 April 2018, Available at: https://www.seapa.org/infographic-malaysias-anti-fake-news-bill/; Article 19, 'Malaysia: 'Anti-Fake News Act' Legal Analysis', April 2018 ('Article 19 Analysis'), Available at: https://www.article19.org/wp-content/uploads/2018/04/2018.04.22-Malaysia-Fake-News-Legal-Analysis-FINAL-v3.pdf

437 Azril Annuar, 'Anti-Fake News Act repealed by Dewan Rakyat again', *Malay Mail,* 9 October 2019, Available at: https://www.malaymail.com/news/malaysia/2019/10/09/anti-fake-news-act-repealed-by-dewan-rakyat-again/1798721; Straits Times, 'Malaysia Parliament passes law to scrap anti-fake news Bill again, abolishing it within the year', 9 October 2019, Available at: https://www.straitstimes.com/asia/se-asia/malaysia-parliament-passes-law-to-scrap-anti-fake-news-law-again-abolishing-it-end-of

438 Anti-Fake News Act 2018 (Act 803)('AFNA'), sections 2, 4, 5, 10, Available at: http://www.federalgazette.agc.gov.my/outputaktap/20180411_803_BI_WJW010830%20BI.pdf

439 AFNA, section 6.

440 See also Article 19 Analysis, pp. 12, 13.

to freely express oneself, or impart and receive information "regardless of frontiers".[441] In its analysis of the AFNA, Article 19 highlighted that extra-territorial application could result in restriction of access of persons based within Malaysia to international sources of information, targeting of news organizations based abroad, and violate the rights to free expression and information of persons based outside of Malaysia.[442]

Oversight and redress and accountability mechanisms provided for under the Act were also limited. Section 7 of the AFNA provided the courts with broad powers to order the removal of any "fake news". Failure to comply with such an order was then punishable under section 7(6) with a fine of up to RM 100,000 (approx. USD 24,252). The Act did not expressly provide that courts must give due consideration to the protection of the rights to free expression or information in such determination.[443] Section 8 of the AFNA provided that persons affected by a section 7 removal order can appeal to set aside such an order within 14 days – this right to appeal however did not extend to any "publication containing fake news which is prejudicial or likely to public order or national security".[444] As was evident in earlier cases of misuse of the Sedition Act and CMA in Malaysia to censor information in the interests of "public order" or "national security", the terms were again left undefined in the AFNA, and provisions were not included within the Act to ensure that limitations on free expression and information could only be applied when strictly necessary for a legitimate and aim and in a proportionate manner.[445]

In August 2018, the new Pakatan Harapan coalition government pushed a bill to repeal the AFNA through the lower house of the Parliament, which was, a month later, rejected by the opposition-dominated upper house.[446] In April 2019, Prime Minister Dr Mahathir Mohamad promised that the government would repeal the AFNA, noting that it was "a law that

441 AFNA, section 3(2).
442 Article 19 Analysis, p. 16.
443 AFNA, section 7.
444 AFNA, sections 8(1), 8(3).
445 This was also noted by the UN Special Rapporteur on freedom of expression in his communication with the Malaysian government, which noted concerning provisions in the Sedition Act and CMA, amongst other laws restricting free expression, and urged the government to "take all necessary measures to ensure (the) repeal" of the AFNA, Communication No. MYS 6/2018 from UN Special Rapporteur on freedom of expression to the Government of Malaysia, 28 December 2018, Available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24287
446 Joseph Sipalan, Praveen Menon, 'Malaysia opposition blocks repeal of 'fake news' law in challenge to Mahathir', *Reuters,* 12 September 2018, Available at: https://www.reuters.com/article/us-malaysia-politics-fakenews/malaysia-opposition-blocks-repeal-of-fake-news-law-in-challenge-to-mahathir-idUSKCN1LS0WO

prevents people from airing their views" which "the government itself may abuse… as happened with the last government… to make use of the law… to create fake news in order to sustain itself."[447] In October 2019, the bill to repeal the AFNA was brought before the Parliament a second time and passed.[448] The AFNA nonetheless remains a prime example of this new generation of flawed legislation that could be utilized to suppress speech.

Singapore

In October 2019, the **Protection from Online Falsehoods and Manipulation Act (POFMA)** came into effect in Singapore.[449] The law was adopted despite concerns highlighted by the ICJ and others, including technological companies, media practitioners, journalists, lawyers, independent publishers, arts organizations, academics, politicians and human rights organizations that it could result in highly excessive government control and restriction of information online in violation of the rights to free expression and information.[450]

447 Bernama, 'Government can handle fake news even without Anti-Fake News law – Mahathir', Prime Minister's Office, 9 April 2019, Available at: https://www.pmo.gov.my/2019/04/government-can-handle-fake-news-even-without-anti-fake-news-law-mahathir/

448 For a bill that is retabled, repeal can be effected even if the upper house rejects it, as the upper house can be bypassed under Article 68 of the Federal Constitution. Notably, in a report released in November 2019, Freedom House noted that the change of government was a factor in recent improvement in internet freedom in Malaysia, even as increased online harassment and criminal prosecutions of online expression, particularly on social media, posed threats to gains. See Freedom House, Freedom on the Net 2019: Malaysia, Available at: https://www.freedomonthenet.org/country/malaysia/freedom-on-the-net/2019

449 Tham Yuen-C, 'Singapore's fake news law to come into effect Oct 2', *Straits Times,* 1 October 2019, Available at: https://www.straitstimes.com/politics/fake-news-law-to-come-into-effect-oct-2; It was brought into force with four subsidiary legislation supplements, detailing selected exemptions for certain services provided by tech companies, including Baidu, Google, Twitter, WeChat and Facebook, Available at: https://sso.agc.gov.sg/SL-Supp/S664-2019/Published/20191001?DocDate=20191001; https://sso.agc.gov.sg/SL-Supp/S663-2019/Published/20191001?DocDate=20191001; https://sso.agc.gov.sg/SL-Supp/S662-2019/Published/20191001?DocDate=20191001; https://sso.agc.gov.sg/SL-Supp/S661-2019/Published/20191001?DocDate=20191001.

450 ICJ, 'Singapore: Parliament must reject internet regulation bill that threatens freedom of expression', 4 April 2019, Available at: https://www.icj.org/singapore-parliament-must-reject-internet-regulation-bill-that-threatens-freedom-of-expression/; Thum Ping Tjin, Kirsten Han, 'Singapore's "Fake News" Bill: The FAQ', *New Naratif,* 9 April 2019, Available at: https://newnaratif.com/research/singapores-fake-news-bill-the-faq/; Asia Internet Coalition, 'Statement on the Singapore Protection from Online Falsehoods and Manipulation Bill', 1 April 2019, Available at: https://aicasia.org/2019/04/01/aic-statement-on-the-singapore-protection-from-online-falsehoods-and-manipulation-bill-1-april-2019/; Yahoo News Singapore, 'Singapore media practitioners voice concerns over proposed fake news law', 18 April 2019, Available at: https://sg.news.yahoo.com/singapore-media-practitioners-voice-concerns-proposed-fake-news-law-030735076.html; 'Journalists Call for Withdrawal of Singapore's "Fake News" Bill', 24 April 2019, Available at: https://docs.google.com/document/d/16pVee1fGx9cU6qADARrgfTtcV60-tVFpm46UGF1-j0o/edit; Harpreet Singh Nehal SC, 'Strengthening the Online Falsehoods Bill: Some Practical Suggestions', April 2019, Available at: https://www.singaporelawwatch.sg/Portals/0/1904-02%20Online%20Falsehoods%20Bill.pdf?fbclid=IwAR3_mN8yJRpaYLnK38U2eWO78Z1qim7-1N6ahOlMxnM9KAKRfHeIMb4x6KY; 'Joint statement regarding the Protection from Online Falsehoods and Manipulation Bill', Available at: https://docs.google.com/document/d/1yNCUHvJBOkZG_WbNt1W_8BAxzHKIjIBK1EJbMLu9Rr8/edit?fbclid=IwAR0uND0exPTHnzvgWiuxHhL75gccbUaCBU-7ZOA4IZSJ8EVMtwydsurxSIc#heading=h.gjdgxs; Adrian Lim, 'NMPs suggest 4 amendments to fake news Bill, including having independent council to review

Prior to the passage of the POFMA, in April 2019, the ICJ addressed a letter to the Prime Minister, Deputy Prime Ministers, Minister for Law and Speaker of Parliament highlighting key concerns in the Act that needed to be addressed by the Singapore government.[451] Similar to the concerns identified with *Malaysia's* AFNA, this law contained vague and overbroad provisions and lacked adequate oversight, redress and accountability mechanisms.

Vague and overbroad provisions prevent precise understanding of the law to enable individuals to regulate their conduct accordingly, in contravention of the general principle of legality. The Act, brought into force to "prevent the electronic communication of false statements of fact", fails to provide a sufficient definition of "false statement of fact" under section 2, which allows for potentially any form of communication – written, visual, audio or otherwise – to be targeted under the law.[452] Section 7 criminalizes the communication of any "false statement of fact" where such communication is likely to "be prejudicial to the security of Singapore, to public health, public safety, public tranquility", "influence the outcome of an election", "incite feelings of enmity, hatred or ill-will" or "diminish public confidence in the performance of any duty or function of, or in the exercise of any power by, the Government, an Organ of State, a statutory board.", This provision fails to define or circumscribe the categories "public safety", "public tranquility" and "public interest".[453]

Wide-ranging discretion is also conferred on ministers and government authorities under the POFMA in their administration of the Act and there are insufficient independent oversight measures to protect against arbitrary or abusive implementation. Parts 3 to 7 of the POFMA provide for powers granted to ministers to "correct" or "stop" the circulation of an alleged "false statement of fact", and to order internet intermediaries to "block" or "disable" access to online locations or "disallow" its services from being used to disseminate

Govt decisions', *The Straits Times,* 30 April 2019, Available at: https://www.straitstimes.com/politics/nmps-suggest-four-amendments-to-draft-fake-news-law-including-having-independent-council-to?fbclid=IwAR1T1l5yxVd4XLqbyjMpWYcWZlTdnxxJPgGuZss83TRw5IRr36yYuwrMPvs; Johannes Tjendro, 'Academics raise concerns on proposed online falsehoods laws; MOE assures research unaffected', *Channel News Asia,* Available at: https://www.channelnewsasia.com/news/singapore/academics-raise-concerns-on-proposed-online-falsehoods-laws-moe-11446818

451 The ICJ did not receive a response to the letter. See ICJ, 'Singapore: ICJ calls on government not to adopt online regulation bill in current form', 12 April 2019, Available at: https://www.icj.org/singapore-icj-calls-on-government-not-to-adopt-online-regulation-bill-in-current-form/

452 Protection from Online Falsehoods and Manipulation Act 2019, Bill No. 10/2019 ('POFMA'), Available at: https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf; See ICJ, 'Legal Briefing: Protection from Online Falsehoods and Manipulation Bill No. 10/2019', 12 April 2019 ('ICJ Legal Briefing'), p. 4, Available at: https://www.icj.org/wp-content/uploads/2019/04/Singapore-online-regulation-bill-briefing-advocacy-open-letter-2019-ENG.pdf

453 ICJ Legal Briefing, p. 5.

alleged "false statements of fact". Government authorities can also control the flow of information through digital advertising or internet intermediaries through "codes of practice" which "give prominence to credible sources of information".[454] The first stage of recourse available to an aggrieved party is ministerial review of a direction or order made under the law – by the minister who made the order in question in the first place, raising concerns regarding the independence of such review and, concomitantly, the right of aggrieved parties to prompt and effective remedy, including judicial remedy.[455] The law also fails to provide clear protections for freedom of expression and information or include exceptions or defences, including the defences of public interest, honest mistake, parody and/or artistic merit. There is no recourse available for a direction or order made under the bill to be quashed on judicial review grounds of illegality, irrationality and procedural impropriety.[456]

A range of imprisonment terms and hefty fines may be imposed under the POFMA as penalties for alleged "false statement of fact", a category that can be interpreted in an overbroad manner to, for example, include individuals or nonindividuals who 'like', 'share' or 'comment' on such information on social media. In addition, intermediaries facilitating communication of such statement may also be held liable. This can result in a chilling effect on the free communication of opinions or other information, particularly in the context of discussions about matters of public interest and concern. Penalties include up to S$100,000 (approx. USD 73,000) or ten years' imprisonment or both for individuals and fines of up to S$1 million (approx. USD 730,000) for non-individuals, and continuing fines of up to S$100,000 per day (approx. USD 73,000) or part of day of a "continuing offence", where "part of day" is not clearly defined, can be imposed on parties deemed to have violated the law.[457]

As with *Malaysia's* AFNA, the POFMA allows for extra-territorial application of penalties on individuals or non-individuals "whether in or outside of Singapore", inconsistent with obligations to protect free expression and information "regardless of frontiers" and which can violate the rights of persons not only in Singapore but also outside of Singapore.[458]

454 POFMA, sections 48(2)(b), 48(2)(c).
455 ICJ Legal Briefing, pp. 6, 7.
456 ICJ Legal Briefing, pp. 11, 12.
457 ICJ Legal Briefing, pp. 8 to 11.
458 ICJ Legal Briefing, pp. 12, 13.

In his Communications to the Singapore government on the POFMA, the UN Special Rapporteur for freedom of expression highlighted serious concern that the law would "not only serve as a basis to deter fully legitimate speech, especially public debate, criticism of government policy and political dissent" but also "serve as a model for far-reaching restrictions on vague and discretionary grounds of falsity".[459]

Case of ***Brad Bowyer***

In November 2019 – in the first reported case of the use of POFMA – **Brad Bowyer**, a member of a political opposition party, was ordered by the POFMA Office to issue a correction notice to a post he had made on Facebook less than two weeks before, in which he had reportedly questioned the independence of two government-linked companies, Temasek Holdings Pte. Ltd and GIC Pte. Ltd[460] and raised concerns on their investment strategies.[461]

The Correction Direction had been issued to Bowyer following an instruction from the Minister of Finance, on the basis that "*(The) post contains clearly false statements of fact, and undermines public trust in the Government. … It is necessary to state this for the record: GIC and Temasek operate on a commercial basis, and the Government is not involved in their individual investment decisions"*.[462]

Within a day of being issued the direction, Bowyer posted a correction notice on his Facebook post. He further noted that *"I am not against being asked to make clarifications or corrections especially if it is in the public interest… (I)n general, I caution all those who comment on our domestic politics and social issues to do so with due care and attention especially if you speak from any place of influence"*.[463]

459 Communication No. SGP 3/2019 from UN Special Rapporteur on freedom of expression to the Government of Singapore, 24 April 2019, Available at: https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_SGP_3_2019.pdf

460 PM Lee Hsien Loong is Chairman of the Board of GIC Pte. Ltd and his wife Ho Ching is the Executive Director and CEO of Temasek Holdings Pte. Ltd. See https://www.gic.com.sg/about-gic/governance/board-of-directors/; https://www.temasek.com.sg/en/who-we-are/our-leadership.html.

461 Channel News Asia, 'POFMA Office directs Brad Bowyer to correct Facebook post in first use of 'fake news' law', 25 November 2019 ('CNA, 25 November 2019') Available at: https://www.channelnewsasia.com/news/singapore/brad-bowyer-facebook-post-falsehood-pofma-fake-news-12122952; Tham Yuen C, 'Govt invokes fake news law for first time, asks opposition member Brad Bowyer to correct Facebook post on Temasek, GIC', *Straits Times,* 25 November 2019 ('Straits Times, 25 November 2019'), Available at: https://www.straitstimes.com/singapore/pofma-office-directs-opposition-member-brad-bowyer-to-add-correction-notice-to-facebook

462 CNA, 25 November 2019.

463 CNA, 25 November 2019.

The use of POFMA against an opposition party member in the lead-up to general elections in Singapore raises a concern that the law will be used to target individuals who express critical dissent. In the case of Bowyer, the Ministry of Finance did not explain how "public safety" or "public tranquility" were threatened by his statement, or provide clarity as to how the government determines that statements "diminish public confidence". His comments could have been adequately countered by a statement of clarification by relevant government agencies. Bowyer's claim about the independence of the companies was an opinion that should have been allowed to be freely rebutted or challenged as a matter of public interest.[464]

Singaporean observers noted that the use of POFMA here drew more attention to what would have remained an obscure post by an opposition politician suggesting that the targeting of Bowyer might have been intended as a message to the general population that the POFMA could be used on politically-linked discussions ahead of the general elections.[465]

Philippines

In July 2019, the **'Anti-False Content' Bill** ('AFC Bill') was introduced in the Senate to "protect the public from any misleading or false information that is being published and has become prevalent on the Internet", noting the State's commitment to "counteract concomitant prejudicial effects to public interest while remaining cognizant of the people's fundamental rights to freedom of speech and freedom of the press".[466]

Provisions in the AFC Bill are similar to those of *Malaysia's* AFNA and *Singapore's* POFMA, allowing government authorities to have wide powers to determine and control what kinds of information are permitted online. Section 5 of the AFC Bill thus allows for the Department of Justice's (DOJ) Office of Cybercrime to order individuals, administrators of online accounts and online intermediaries to "rectify", "take down'" or "block access" to any information that would "tend to mislead the public".[467] The bill provides no guidance as to how DOJ officers are to make the determination of whether a piece of information should be permitted or regulated online, and makes no mention of the rights to free expression and information. Information

464 Also expressed in ICJ communications with partners.
465 ICJ communications with partners.
466 'Act Prohibiting the Publication and Proliferation of False Content on the Philippine Internet, Providing Measures to Counteract its Effects and Prescribing Penalties Therefor' ('AFC Bill'), Available at: https://senate.gov.ph/lisdata/3022527054!.pdf
467 AFC Bill, section 5.

that can be removed includes "matters affecting the public interest".[468] "Public interest" is also vaguely defined as "anything that affects national security, public health, public safety, public order, public confidence in the Government, and international relations of the Philippines".[469]

Overbroad provisions make it difficult for the law to provide clear guidance for individuals to regulate their conduct accordingly. Nearly any form of online communication is subjected to prosecution under section 3 of the AFC Bill, which covers any "act of uploading content on an online intermediary with an intent to circulate particular information to the public", where such content can be "text, image, audio recording, video or animation".[470] The only factor determining whether a post online is criminal under the bill is whether content was circulated "knowing or having a reasonable belief that it is false or that would tend to mislead the public." – there is no clarification on what "mislead(ing) the public" entails, and the bill punishes not only the person posting such content, but also anyone offering or providing services to assist or finance the creating or publishing of such content.[471] This allows for penalties to potentially affect online intermediaries, including social media services, search engine services, online messaging services, and online video and audio-sharing services.[472]

Similar to *Singapore's* POFMA, this bill does not provide for adequate redress or accountability mechanisms and in fact tasks the same body who implements the bill with also reviewing and overseeing its implementation. It does not allow for judicial review of "rectification", "take down" or "access blocking" orders and instead provides, under section 6, for an aggrieved party to "file a petition for review" with the DOJ within 15 days of an order, the same authority which issues such orders.[473]

Severe penalties are provided for under the bill – an individual can face up to six years' imprisonment and fined up to PHP 500,000 (approx. USD 9,826) for publishing violative content, and up to 12 years' imprisonment and fined up to PHP 2 million (approx. USD 39,295) for financing the creation or publication of such content.[474] The bill also allows for extra-territorial

468 *Ibid.*
469 AFC Bill, section 3(d).
470 AFC Bill, sections 3(a), (b).
471 AFC Bill, sections 4(a), (c), (d).
472 See also Human Rights Watch, 'Philippines: Reject Sweeping 'Fake News' Bill', 25 July 2019, Available at: https://www.hrw.org/news/2019/07/25/philippines-reject-sweeping-fake-news-bill?fbclid=IwAR0hQJrQ3KzKLz0ac96mYnny09F0L5AGZa8Kx-gcRhSHRrelcN8XNvOR7g8
473 AFC Bill, section 6.
474 AFC Bill, section 8.

application to Filipino nationals posting information online outside of the Philippines.[475]

Lao PDR

In July 2019, Laos' Ministry of Information, Culture and Tourism issued a **government order** requiring all administrators of news and information-sharing groups on social media platforms to register with the ministry's media departments, towards "controlling the spread of fake news and disinformation on social media".[476] In announcing the order, the Director-General of the ministry's Mass Media Department noted that this regulation would operate in line with Laos' **Law on Prevention and Combating Cyber Crime 2015** ('Law on Cybercrime'), which under article 8 criminalizes the "causing of damages via online social media" with up to three years' imprisonment and a fine of up to 20 million Kip (approx. USD 2,290).[477] Social media platforms must also operate in accordance with the **amended Media Law of 2008**, enacted in 2016, to "ensure that the media implements their duties … to be a sharp voice of the (ruling Lao People's Revolutionary) Party and the people in order to propagate the guidelines and directions, and laws and social-economic development plans of the State".[478]

Lack of clarity about how the government order will be imposed in practice and the Lao government's track record in clamping down on freedom of expression, whether online or otherwise, raise serious concerns that this new order will effectively further curtail independent reporting and information online. This risk is intensified by the Media Law, which provides for near-absolute State control of the media,[479] and the Law on Cybercrime. This Law provides for criminal liability for overbroadly conceived "offences" such as "causing of damages via online social media" which includes the

475 AFC Bill, section 9.
476 Richard Lipes, 'Laos Moves to Register Private Online News Sites in a Bid to Control 'Fake News'', *Radio Free Asia,* 19 July 2019, Available at: https://www.rfa.org/english/news/laos/register-07192019160935.html; Souksakhone Vaenkeo, 'Ministry orders registration of social media news platforms in Laos', *Asia News Network*, 16 July 2019, Available at: http://annx.asianews.network/content/ministry-orders-registration-social-media-news-platforms-laos-100198
477 Ibid.; Law on Prevention and Combating Cyber Crime 2015 (No. 61/NA)('Law on Cybercrime'), articles 8, 13, 62(5), English translation available at: https://www.laocert.gov.la/ftp_upload/Cyber_Crime_Law_EnVersion.pdf
478 Vientiane Times, 'Social media platforms yet to register as required by law', 10 August 2019, Available at: http://www.vientianetimes.org.la; Ounkeo Souksavanh, Roseanne Gerin, 'Lao Lawmakers Approve Restrictive Amendment to Media Law', *Radio Free Asia,* 10 November 2016, Available at: https://www.rfa.org/english/news/laos/lao-lawmakers-approve-restrictive-amendment-to-media-law-11102016153123.html
479 Southeast Asian Press Alliance, '[Laos] Critical cyberspace shrinks, mainstream press further muted', 3 May 2017, Available at: https://www.seapa.org/wpfd2017-critical-cyberspace-shrinks-mainstream-press-further-muted/

defamation-type offence of "slandering, blaspheming or using impolite words", using computer data and information to "destroy national security, peace and order in society, national culture and fine traditions of the nation" and the "convening, persuading or encouraging of people to separate national solidarity".[480]

viii. Laws which aim to protect cybersecurity

Laws and regulations ostensibly designed to protect cybersecurity have also been adopted – significantly expanding government control of the online sphere through legalizing government monitoring and regulation of online information systems, electronic data and networks, technological companies and intermediary bodies. These cybersecurity laws again adopt the objective of protecting "national security" to justify problematic provisions which could be used to suppress expression on a more widespread and systematic manner than older laws. This is evident in *Vietnam, Thailand* and *Cambodia*.

The protection of national security is a legitimate purpose for the restriction of freedom of expression and information, but any restriction must be strictly necessary and proportionate to that legitimate aim.[481] What we instead see in Southeast Asia, is the crafting of legal frameworks purportedly to address legitimate security interests which may in certain respects provide for strong regulatory measures against threats to security in the cybersphere, but do not comport with the requirements of necessity and proportionality. They incorporate problematic provisions which are not human rights compliant and allow for further infringement of the rights of individuals online.

The UNGPs oblige States to enact effective laws, regulations and policies to ensure that ICT companies and other corporate internet service providers duly respect and protect human rights in the provision of their services.[482] While appropriate oversight and regulation of ICT companies and cyberspace is, therefore, necessary, the laws covered below will reflect that measures taken in the region raise risks of further rights violations online – of free expression, information and privacy – rather than strengthening protections against these violations.

480 Law on Cybercrime, articles 13(1), 13(3), 13(4).
481 See Section II (ii).
482 See Section II (v).

Vietnam

In January 2019, Vietnam's **Law on Cybersecurity** ('LOCS') came into effect to "protect national security" and "ensure social order and safety on cyberspace."[483] Reporters Sans Frontières commented that the law introduced a "totalitarian model of control of information".[484] The law codified and expanded upon provisions in an earlier 2013 regulation, **Decree No. 72 on the management, provision and use of Internet services and online information** ('Decree No. 72') which allowed for State control of "management, provision and use of Internet services and online information" to "prevent the abuse of the Internet to affect national security and social order, fine traditions and customs".[485]

In November 2018, the Ministry of Public Security (MPS) released a **Draft Decree Implementing the Law on Cybersecurity** ('Draft Decree'), clarifying that the law would protect against cyber-attacks and combat "hostile and reactionary forces" who utilize the internet "against the State".[486] At least two organizations representing internet and technology companies, however, noted during a public consultation process that the law could in fact undermine cyber and data security, as its provisions – particularly on data localization – could be "technically infeasible", "disrupt global data flows", harm the country's digital economy, and "create additional entry points into Vietnam's IT systems for cyber criminals".[487] Although these were arguments put forth by commercial entities representing industrial interests rather than specific human rights concerns, they highlighted gaps in the Vietnamese government's argument that its legal measures would

483 Kim Loan, 'Ten laws to come into effect from January 1, 2019', *VGP News,* 27 December 2018, Available at: http://news.chinhphu.vn/Home/Ten-laws-to-come-into-effect-from-January-1-2019/201812/35550.vgp

484 RSF also noted that the LOCS appeared strongly influenced by repressive regulations in China which govern the internet. See 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

485 English translation of Decree No. 72/2013/ND-CP of July 15, 2013, on the management, provision and use of Internet services and online information, Available at: https://vnnic.vn/sites/default/files/vanban/Decree%20No72-2013-ND-CP.PDF

486 This was reportedly stated by the ministry in a Question-and-Answer session in October with lawmakers. See Agence France-Presse, 'New year, new repression: Vietnam imposes draconian 'China-like' cybersecurity law', *South China Morning Post,* 1 January 2019, Available at: https://www.scmp.com/news/asia/southeast-asia/article/2180263/new-year-new-repression-vietnam-imposes-draconian-china

487 Asia Internet Coalition, 'Comments on the Draft Decree Guiding the Implementation of Law on Cybersecurity', 13 December 2018 ('AIC, 13 December 2018'), Available at: https://aicasia.org/wp-content/uploads/2018/12/AIC_Comments-on-Draft-Decree-11122018-edited.EN-final.pdf; The Software Alliance, 'BSA Comments on the Draft Decree Implementing Law on Cybersecurity', 13 December 2018 ('BSA, 13 December 2018'), Available at: https://www.bsa.org/files/policy-filings/12142018BSA_Position_Paper_on_Draft_Decree_implementing_Law_on_Cybersecurity_%20ENG.pdf

effectively protect national (cyber)security. The groups' concerns were not adequately addressed following the consultation process.

Vague and overbroad provisions in the LOCS protecting "national security", "public order" and against "propaganda" or "defamation" are very similar to provisions in Vietnam's Penal Code which have been used systematically to clamp down on any information deemed unwelcome by the authorities, including those critical of the government.[488] The law "severely sanctions" any use of cyberspace in a manner "not prejudicial to national security, social order and safety", and clearly designates cybersecurity protection to be "subject to the leadership of the Communist Party of Vietnam and the consistent governance by the State, to mobilize the synergic strength of the political system" under article 4(2).[489] Articles 8 and 15 include wide-ranging prohibitions on "producing, posting or dispersing any information" that, *inter alia*, constitutes "propaganda against the State" which "distorts or defames the people's government", "instigates violent disturbances, disrupts security or public order", "offends the nation, national flag, national emblem, national anthem, great people, great leaders, famous persons or national heroes", "distorts the history or negates a revolution achievement", "sabotages the fine customs and practices of the nation (or) social morality" or are "embarrassing or slanderous" and "offends any person's dignity or honour". Article 26 prohibits "websites, web portals or specialized pages on social networks of agencies, organizations and individuals" from "providing, posting or transmitting any information prejudicial to national sovereignty and security".[490]

The LOCS goes beyond older modalities employed by State authorities to control online information and expression, and seeks to compel internet and technological companies, at risk of legal sanctions, to assist and support the State in online censorship. The law covers all "(l)ocal and foreign agencies and entities, when providing services on cyberspace or owning any information systems in Vietnam" – applying to any and all companies involved in a broad spectrum of online activities which is not limited to social media services, but can also include entities such as online accommodation booking services, online shopping portals, media services providers or banks

488 See Section III (iv).
489 Law on Cybersecurity, articles 2 to 5. The full text of the Law on Cybersecurity is not available in English. However, the latest draft is available at: file:///C:/Users/User/Desktop/ICJ%20DS/2018/VIETNAM/Draft%20Law%20on%20Cybersecurity%20-%2018th%20version%20-%20ENG.pdf
490 Law on Cybersecurity, article 26.

which provide online banking services.[491] Article 26 provides that companies must "set up mechanisms to authenticate information when users register digital accounts", "delete or prevent" any information published on their networks or information systems deemed in violation of the law "within 24 hours", and "cease to provide services on the telecommunication works or the internet" to any person who posts such alleged illegal content.[492] The law further dictates that companies must provide data on their users "when required" to MPS' "specialized force in charge of cybersecurity protection" or "competent authorities" under the MIC – in violation of the users' right to privacy – and "implement requirements from the competent authorities in investigating and sanctioning violations", regardless of whether such requirements may infringe on human rights such as freedom of expression and information.[493] The law also permits the MPS to conduct "cybersecurity audits" to monitor compliance.[494]

The LOCS is also problematic because it compels data localization – requiring companies to "store in Vietnam the personal information of the service users in Vietnam and important data related to national security" and "locate their head offices or representative offices in Vietnam", where the "(g)overnment shall detail what types of information shall be stored in Vietnam and which enterprises are required to locate their head offices or representative offices in Vietnam".[495] These requirements are vague and do not guarantee that confidential personal information belonging to users will not be provided in violation of their rights to privacy and security, and are left open to the unfettered discretion of State authorities.[496] Asia Internet Coalition, a coalition representing internet companies on matters of public policy, further highlighted that data localization would not ensure data confidentiality, as proposed by policy makers and in fact "potentially create a focal target for cyber-attacks and consequently make Vietnam more vulnerable in terms of cyber security".[497]

491 Law on Cybersecurity, article 26(2); See also Duane Morris, 'Vietnam's new Cybersecurity Law: A headache in the making?', July 2018 ('Duane Morris, July 2018'), Available at: https://www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf
492 Law on Cybersecurity, articles 26(2)(a), (b) and (c).
493 Law on Cybersecurity, articles 26(2)(a), (b), (c), (dd).
494 Law on Cybersecurity, articles 12, 24.
495 Law on Cybersecurity, articles 26(2)(d), 26(3).
496 Duane Morris, July 2018.
497 "In most instances, data localization mandates do not increase commercial privacy nor data security.Therefore, it is important to recognize that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely. Data security depends on the technical, physical, and administrative controls implemented, regardless of where the data is stored." See AIC, 13 December 2018, p6.

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, and there is no provision for appeal or judicial review of orders made by the MPS or MIC under the law.[498]

The LOCS will likely become another legal tool misused by the Vietnamese government to clamp down on expression and information online.[499] Indeed, the law came into force in the midst of increased efforts by the State to control online discourse, including through a crackdown on human rights defenders, activists and independent bloggers.[500]

In July 2017, Vietnam's Minister of Information and Communications (MIC) reportedly stated that his ministry had successfully requested technological companies Google and Facebook to remove "3,367 clips with bad and poisonous content" and "more than 600 accounts that have violating content"[501], and in December 2017, a military cyber unit, 'Force 47', was set up with approximately 10,000 persons tasked to monitor the internet and "combat erroneous views" and "wrongful opinions" expressed online about the government.[502] In December 2018, the Journalists' Association of Vietnam introduced a new code of conduct for social media use, prohibiting its member journalists from posting news, images or comments that "run counter to" the State.[503]

498 BSA The Software Alliance also noted this in its comments to the Vietnamese government during a public consultation on the Draft Decree, See BSA, 13 December 2018.

499 Notably, in May 2018, it was reported that Nguyen Thanh Hong, a member of the committee in the National Assembly coordinating the review of the LOCS, himself conceded that "it won't be right to say that the law will not affect the interests of organizations and individuals… (b)ut there has to be a choice made between national security interests and the protection of people's legal rights versus personal freedom and the right to use the internet." See Bao Ha, 'Cyber security law restrictions worry Vietnamese legislators', *VN Express International*, 29 May 2018, Available at: https://e.vnexpress.net/news/news/cyber-security-law-restrictions-worry-vietnamese-legislators-3756271.html

500 See Section III (iv).

501 Human Rights Watch, 'Vietnam: Withdraw Problematic Cyber Security Law', 7 June 2018 ('HRW, Vietnam Cyber Security Law'), Available at: https://www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law; Referring to [Vietnamese] Khôi Nguyên, 'Google và Facebook tiếp tục gỡ bỏ, ngăn chặn thông tin xấu độc', *Báo Moi*, 14 July 2017, Available at: https://baomoi.com/google-va-facebook-tiep-tuc-go-bo-ngan-chan-thong-tin-xau-doc/c/22753780.epi

502 HRW, Vietnam Cyber Security Law; Referring to [Tiếng Việt] Thời Sự, 'Hơn 10.000 người trong 'Lực lượng 47' đấu tranh trên mạng', *Tuổi Trẻ*, 25 December 2017, Available at: https://tuoitre.vn/hon-10-000-nguoi-trong-luc-luong-47-dau-tranh-tren-mang-20171225150602912.htm; James Hookway, 'Introducing Force 47, Vietnam's New Weapon Against Online Dissent', *Wall Street Journal,* 31 December 2017, Available at: https://www.wsj.com/articles/introducing-force-47-vietnams-new-weapon-against-online-dissent-1514721606

503 Associated Free Press, 'Vietnam's cyber-security law takes effect amid criticism', *Straits Times,* 2 January 2019, Available at: https://www.straitstimes.com/asia/vietnams-cyber-security-law-takes-

Stringent obligations placed on internet and technological companies under the LOCS also increase risks that companies may adopt measures in contravention of the rights to privacy, free expression and information in order to protect themselves from government sanctions. In June 2019, the MIC reportedly warned users and companies to refrain from placing advertisements on videos hosted by YouTube which allegedly promote "anti-State propaganda", noting that it had found approximately 55,000 "harmful" YouTube videos, of which 8,000 were removed following requests from Vietnamese authorities.[504] Meanwhile, in its Transparency Report, Facebook noted that in the last six months of 2018, it had restricted 1,553 posts and three profiles in Vietnam as opposed to 265 "restrictions" in the six months prior, and only 22 "restrictions" in the last six months of 2017. Facebook noted that while the 2017 "restrictions" had been made pursuant to "private reports related to defamation", "restrictions" in 2018 were made mostly "in response to reports" from the MPS and MIC, and "restrictions" in the latter half of 2018 largely "related to content alleged to violate Decree No. 72/2013/ND-CP, including *anti-state content*, *defamation of public officials*, and the *spread of false information*."[505] (emphasis added)

These figures do not show the exact content Google's YouTube and Facebook removed. The data does reflect how ICT companies can face increased pressure to remove data from their platforms through the wielding of laws targeting cybersecurity – such as was the case with Decree No. 72 – and intensifies concerns that the LOCS can be misused in a similar manner.[506]

It is evident that although Vietnam promulgated the LOCS to enhance cybersecurity, its provisions focus more on content regulation and narrowing the exercise of free expression and information online by individual internet users. For instance, it obliges private ICT companies to enforce such limitations in line with the Vietnamese government – outsourcing regulatory capacity to private companies which may lack accountability.[507]

effect-amid-criticism

504 James Pearson, 'Vietnam ramps up pressure on Google's YouTube advertisers', *Reuters,* 12 June 2019, Available at: https://www.reuters.com/article/us-vietnam-cyber-google/vietnam-ramps-up-pressure-on-googles-youtube-advertisers-idUSKCN1TD0FC

505 Data available at: https://transparency.facebook.com/content-restrictions/country/VN

506 In April 2018, more than 50 Vietnamese human rights activists and independent media groups addressed an open letter to Mark Zuckerberg, the Chief Executive Officer of Facebook Inc., alleging that "after (the) high-profile agreement to coordinate with a government that is known for suppressing expression online and jailing activists, the problem of account suspension and content takedown has only grown more acute". See Mai Nguyen, 'Vietnam activists question Facebook on suppressing dissent', *Reuters,* 10 April 2018, Available at: https://www.reuters.com/article/us-facebook-privacy-vietnam/vietnam-activists-question-facebook-on-suppressing-dissent-idUSKBN1HH0DO

507 Report of the Special Rapporteur on the promotion and protection of the right to freedom of

Appropriate cybersecurity legislation should have, at the very least, avoided reproducing and incorporating existing vague and overbroad provisions from the Penal Code, such as "propaganda" or "defamation" (which should not be criminalized). The process should have involved a multi-stakeholder review and input into the drafting process –from ICT companies, civil society, academics and technical experts.

Thailand

In May 2019, the **Cybersecurity Act B.E. 2562 (2019)** ('Cybersecurity Act') came into force in Thailand. It was passed by the National Legislative Assembly without opposition[508], despite concerns raised by civil society, academics, opposition politicians and internet companies that the law's overbroad provisions and lack of oversight and accountability mechanisms allowed for potential government abuse of power to mass surveil private data and online communications.[509]

In September 2019, non-governmental organization Manushya Foundation published a report detailing difficulties and deficiencies evident in the Act and proposed a series of recommendations following consultations with academics, digital rights advocates, civil society and the government sector.[510] These pertained to overbroad, undefined provisions which allowed for overly expansive exercise of executive authority in implementing the Act, intrusive surveillance powers provided to the State to monitor online activity and expression, an absence of checks and balances against the executive in the implementation of the Act and inadequate provisions for remedies in the event of rights violations or abuses.[511]

---

opinion and expression, 6 April 2018, A/HRC/38/35 ('A/HRC/38/35'), para 17.

508 13 votes approved, 16 abstained and none opposed.

509 Patpicha Tanakasempipat, 'Thailand passes internet security law decried as 'cyber martial law'', *Reuters,* 28 February 2019, Available at: https://www.reuters.com/article/us-thailand-cyber/thailand-passes-internet-security-law-decried-as-cyber-martial-law-idUSKCN1QH1OB; Baker and McKenzie, 'Thailand Cybersecurity Act, B.E. 2562 (2019) is Effective', May 2019, Available at: http://bakerxchange.com/rv/ff004c3c7fb28fa5221d901d0f4f9b725497f42f; Tech Crunch, 'Thailand passes controversial cybersecurity law that could enable government surveillance', 28 February 2019, Available at: https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/; Pravit Rojanaphruk, 'Future Forward Seeks To Amend Junta's Cyber Law', *Khaosod* English, 24 September 2019, Available at: http://www.khaosodenglish.com/politics/2019/09/24/future-forward-seeks-to-amend-juntas-cyber-law/

510 The ICJ participated in the Experts' Meeting held by Manushya Foundation in preparation of its report.

511 Manushya Foundation, 'Thailand's Cybersecurity Act: Towards A Human-Centered Act Protecting Online Freedom And Privacy, While Tackling Cyber Threats', September 2019 ('Manushya Foundation 2019 report') Available at: file:///C:/Users/User/Desktop/Manushya%20TH%20Cybersecurity%20Act%20report.pdf

Brought into force to combat "cyber threats" or "hacking attacks", the Cybersecurity Act provides sweeping powers to government authorities to monitor online information, and search and seize electronic data and equipment under an overarching framework of protecting "national security", through protecting against "threats" to the country's "Critical Information Infrastructure" (CII), where "national security" and CII are left vaguely defined.[512] Section 3 of the Act broadly includes as CII "any computer or computer system that the Government Agency or private organization uses in their operations which relate to maintaining national security, public security, national economic security, or infrastructures in the public interest".[513] This allows for arbitrary interpretation by State bodies in implementing the Act including nearly any organization or individual under its remit, and for any purpose deemed to be in the interest of national or public security.

This expanded authority is particularly concerning as the powers extended to State bodies tasked with interpreting and executing the law are not subject to independent monitoring mechanisms or authorities. The Act creates the National Cybersecurity Committee ('NCSC') which sets policy standards for the implementation of the CSA, headed by Prime Minister Prayuth Chan-o-cha and including ministers of the Ministry of Defence, the Ministry of Digital Economy and Society (MDES), the Ministry of Justice and the Ministry of Finance, the Commissioner-General of the Royal Thai Police (RTP) and the Secretary-General of the National Security Council (NSC).[514] It also sets up the Cybersecurity Regulation Committee ('CRC') which – supported by the Office of the National Cybersecurity Committee ('NCSC Office') – implements these standards, led by the MDES and including the Royal Thai Armed Forces and the RTP.[515]

The NCSC possesses, among other powers, the authority to determine three levels of "cyber threats" – "non-critical", "critical" or "crisis" – which pose significant risks and broadly compromise the country's CII.[516] A threat is deemed to be at "critical" or "crisis" levels where it "affects national defence, public safety or order".[517] The NCSC is provided with broad powers

512 [Thai] Cybersecurity Act B.E. 2562 (2019)('Cybersecurity Act'), section 3, Available at: http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF; For reference of English translation of the Act, and related concerns, refer to Manushya Foundation 2019 report.
513 [Thai] Cybersecurity Act, section 3; See also Manushya Foundation 2019 report, p. 17.
514 [Thai] Cybersecurity Act, sections 5, 9, 41 to 43; See also Manushya Foundation 2019 report, pp. 28 to 31.
515 [Thai] Cybersecurity Act, sections 12, 13, 22, 61 to 66; See also Manushya Foundation 2019 report, pp. 28 to 31.
516 [Thai] Cybersecurity Act, section 60(3)(a).
517 [Thai] Cybersecurity Act, section 60; See also Manushya Foundation 2019 report, pp. 22 to 23.

to determine or designate any organization as CII, and also to determine fundamentally what amounts to a "threat" in the first place.[518] The Act also allows for State bodies to implement the law against individuals and entities even without requiring the bodies to furnish sufficient evidence to prove a material risk of harm[519] and in certain cases do not allow for judicial review of decisions by the authorities[520] – in violation of the principles of legitimacy, necessity and proportionality.[521]

The extent of executive discretionary authority is particularly concerning with respect to actions that the State can take where "it appears" that a threat may be "critical" or "crisis" level.[522] At the "critical" level, the CRC can order any legal person for investigation, enter premises, search and seize electronic data and equipment from any private entity, make copies of such data, test electronic equipment or systems.[523] Officials are also empowered to request "real-time" access to information held by private entities.[524] While judicial oversight is present with respect to "non-critical" and certain "critical" threats[525], where a "cyber threat" is deemed to be at "crisis" level, the Secretary-General of the NCSC is authorized to undertake all these actions without obtaining a court warrant, and these decisions are not subject to appeal before the courts.[526] Failure to comply with such orders is punishable with up to three years' imprisonment and beyond tens of thousands of baht (which can accumulate to thousands in USD).[527]

Severe limitations in the Cybersecurity Act allow for potentially egregious violations of the rights to privacy and freedom of expression and information by military-led State authorities under the law. It allows

518 [Thai] Cybersecurity Act, sections 3, 49; See also Manushya Foundation 2019 report, pp. 14 to 15, 18.
519 See Manushya Foundation 2019 report, pp. 19, 20.
520 [Thai] Cybersecurity Act, section 69.
521 [Thai] Cybersecurity Act, sections 61 to 68.
522 [Thai] Cybersecurity Act, sections 61, 64 to 66 apply where it "appears to the CRC that there exist or may exist a 'critical' risk'", the CRC can order the NCSC Office to take relevant action. Section 62 provides for the power of the Secretary-General of the NCSC "in order to analyse and evaluate the damage from (any) cyber threats" to make relevant orders to authorities. For threats at "crisis" level, section 67 allows the NSC to deal with the matter, or in cases of emergency, section 68 allows the Secretary-General to proceed without a court order.
523 [Thai] Cybersecurity Act, sections 66 to 69.
524 [Thai] Cybersecurity Act, section 68(2).
525 Judicial oversight is not extended to some "critical" threats, see [Thai] Cybersecurity Act, section 66, particularly section 66(1)(2).
526 [Thai] Cybersecurity Act, section 68(1). Appeal is only available for "non-critical" threats, see section 69.
527 [Thai] Cybersecurity Act, sections 75, 76; Section 75 imposes a fine of up to THB 300,000 and an increased fine of THB 10,000 per day until an individual or legal person complies with an order, and imposes up to 1 year's imprisonment or a fine of up to THB 20,000 for non-compliance. Section 76 imposes up to three years' imprisonment and a fine of up to THB 60,000 for non-compliance.

for the removal of independent oversight and accountability mechanisms where a "cyber threat" is deemed by those same authorities to be "critical" or "crisis" levels, and for the National Security Council – led by the military – to override provisions of the Act and implement measures under laws governing national security in a "crisis" level situation.[528] The overarching policy governing the implementation of the Act – "national security" – is subject to wide discretionary interpretation by State authorities. Though the Act does state that measures can be imposed "only as necessary", there are no guidelines to govern assessment.[529]

Meanwhile, governance and policy-making standards guiding the determination of what "national security" and what a "national emergency" entails rest squarely within the powers of the present-day government and military regime through the NCSC. Although courts can review orders in certain circumstances, the Act itself does not prescribe an independent body or mechanism with technical expertise to review or hear appeals against orders made by the NCSC.[530] The composition of the NCSC currently includes independent experts from the technological or cybersecurity sector, who have technical expertise but whose powers to ensure that the NCSC exercises its executive power in compliance with human rights standards and law may be limited as they are all appointed by the military-led Cabinet.

The coming into force of the Cybersecurity Act amidst recent measures to increase surveillance of the internet raises serious concerns that it may be abused to curtail online expression and information.[531] In August 2019, the Minister of Digital Economy and Society announced the setting up of an "Anti-Fake News" center and website to combat disinformation, where "(p)eople can submit any news … suspicious of being unauthenticated, or that could incite fear and confusion to the public" which could then be "verified" by government officials "within two hours".[532]

528 [Thai] Cybersecurity Act, section 67; See also Manushya Foundation 2019 report, p. 53.
529 [Thai] Cybersecurity Act, sections 66, 68.
530 Judicial review is permitted, for example, under sections 65, 66 and 69.
531 Notably, the ICJ was informed through communications with its partners that in one case pertaining to *lèse majesté* – a case linked to the Thai Federation movement – the arrested person was asked to sign an agreement that they would not use *lèse majesté* language again, and that the agreement had referred to the power of authorities under the Cybersecurity Act to obtain information from electronic devices.
532 Associated Press, 'Thailand to set up Center to Combat 'Fake News'', *Khaosod English*, 22 August 2019, Available at: http://www.khaosodenglish.com/news/crimecourtscalamity/2019/08/22/thailand-to-set-up-center-to-combat-fake-news/; The legal basis used to set up the center is unclear. Notably NCPO Announcement No. 26/2557 had enabled the Minister of MDES to set up a 'working group' with powers to monitor, suspend and investigate content that may "incite, instigate and harbour violence, a lack of credibility and a lack of respect for the law, or which may be critical of the work of the NCPO". See [Thai] NCPO Announcement No. 26/2557, Available at: https://library2.parliament.go.th/giventake/content_ncpo/ncpo-annouce26-2557.pdf. This announcement

Manushya Foundation has highlighted that there is a risk powers under the Cybersecurity Act may be misused beyond the remit of "cyber threats" to curtail online dissent through the "Anti-Fake News" center as some individuals from the CRC will also oversee the center.[533] In October 2019, the Minister of Digital Economy and Society stated that the government would impose section 26 of the CCA to require owners of cafes to retain log files of the browsing data of their customers for at least three months, so that the data could be utilized by the "Anti-Fake News" center to identify alleged "false and inappropriate" information online.[534] Concerns have been raised that the center, which launched in November 2019, will not only assist the government in censorship and surveillance,[535] unlawfully infringing on the rights to expression, information and privacy of individuals.

Cambodia

In May 2012, the Cambodian government announced that it would initiate the elaboration of a **Cybercrime Law** to guard against ""ill-willed groups or individuals" from "spreading false information" online, to prevent "hacking (of) both government and private data or websites" and ensure "the common interest is protected".[536] Despite calls from civil society in Cambodia for the government to release official drafts of the law to allow concerned stakeholders and wider members of the public to provide comment on the law, the government has neither released official drafts of the law, nor opened it up to public discussion or consultation.[537]

In April 2014, an unofficial first draft of the Cybercrime Law was leaked and widely circulated.[538] In May 2015, the spokesperson for Cambodia's Ministry of Posts and Telecommunications indicated that the law would be

was not repealed by the latest HNCPO Order dated 9 July 2019.

533 Manushya Foundation 2019 report, p. 30.

534 Kate Lamb, 'Thai cafes forced to track customers' wifi use, sparking free speech fears', *The Guardian,* 10 October 2019, Available at: https://www.theguardian.com/world/2019/oct/10/thai-cafes-forced-to-track-customers-wifi-use-sparking-free-speech-fears

535 *Ibid.*

536 Cambodian Center for Human Rights (CCHR), 'CCHR Briefing Note – February 2014 Cyber Laws: Tools for Protecting or Restricting Freedom of Expression?', February 2014, Available at: https://ifex.org/images/cambodia/2014/03/03/cambodia_cyber_crimes_legislation_cchr.pdf; CCHR, 'Cambodian Government is drafting the first ever Cyber Law', 24 May 2012, Available at: https://www.cchrcambodia.org/index_old.php?url=media/media.php&p=alert_detail.php&alid=21&id=5; Joshua Wilwohl, 'Anonymous Hacks Government Websites', *Cambodia Daily,* 13 September 2013, Available at: https://www.cambodiadaily.com/news/anonymous%e2%80%88hacks-government-websites-42250/

537 *Ibid.*, 'Open Letter on current draft laws – To: Ministers of the Royal Government of Cambodia', Available at: https://www.ccimcambodia.org/wp-content/uploads/2014/10/Open_Letter_request_for_draft-laws_EN.pdf

538 CCHR, 'Open Letter from CCHR concerning Draft Cybercrime Law', 28 April 2014 ('CCHR Open Letter'), Available at: https://cchrcambodia.org/media/files/press_release/488_20colccrdcle_en.pdf

used to combat information "insulting, illegally attacking and destroying the honor of the government", and that it would be opened up for public consultation.[539] However, no consultation in fact took place. In September and October 2015, a second draft was leaked and circulated.[540]

The drafts contained numerous problematic provisions, highlighted in an open letter by non-governmental organization Cambodian Center for Human Rights (CCHR), which referred to the first unofficial draft of the Cybercrime Law.[541] First, the draft, under article 28, included vague and overbroad provisions which would prohibit any content deemed to "hinder the sovereignty and integrity of the Kingdom of Cambodia", "incite or instigate the general population that could cause one or many to generate anarchism", "(damage) the moral and cultural values of the society", "generate insecurity, instability, and political cohesiveness", "undermined the integrity of any governmental agencies", or which amounted to "manipulation, defamation, and slanders".[542] Secondly, the draft established, under Chapter II, the creation of a National Anti-Cybercrime Committee ('NACC'), very similar to the NCSC under *Thailand's* Cybersecurity Act, which was not an independent review mechanism to oversee implementation of the law. The NACC would be led by the Prime Minister, and include the Deputy Prime Minister, representatives from the Ministries of Interior, Information, Posts and Telecommunications, Justice and the National Police and operate as a policy and oversight committee, with a General Secretariat that would oversee and ensure enforcement of the law.[543]

The second unofficial draft of the law removed the chapter dealing with the establishment of the NACC and article 28. However, it retained other problematic provisions. Article 27 in the second draft allowed for legal entities, including civil society organizations, to be dissolved for "cybercrimes" committed by individuals within the organizations, which remained broadly defined and subject to abuse.[544] For example, article 13 of the second draft

539 Mech Dara, 'Cyber Law to Protect Gov't Honor, Ministry Says', *Cambodia Daily,* 27 May 2015, Available at: https://www.cambodiadaily.com/news/cyber-law-to-protect-govt-honor-ministry-says-84431/

540 CCHR, 'CCHR Briefing Note – February 2016 Digital Wrongs? An Overview of the Situation of Digital Rights in Cambodia', February 2016 ('CCHR Briefing Note, February 2016') Available at: https://cchrcambodia.org/admin/media/analysis/analysis/english/2016_03_03_CCHR_Briefing_Note_Digital_Wrongs_ENG.pdf

541 See also CCHR Open Letter; CCHR Briefing Note, February 2016, p11.

542 Cybercrime Law Draft V.1 ('Cybercrime Law First Draft'), Article 28, Unofficial English translation available at: https://www.article19.org/data/files/medialibrary/37516/Draft-Law-On-CyberCrime_Englishv1.pdf

543 Cybercrime Law First Draft, Chapter II.

544 CCHR Briefing Note, February 2016, p12.

criminalized the "obtaining of any data considered to be confidential and which are specifically protected against unauthorized access" – which neither included protections for individuals who had received such information by mistake, nor protected against content released in the public interest, such as information gleaned from journalistic reporting.[545] The second draft further provided, as with *Thailand's* Cybersecurity Act, for broad powers for the police to investigate "cybercrimes", search and seize property of suspect individuals, and failed to ensure independent and impartial oversight or procedural safeguards.[546]

Cambodia's efforts to draft a Cybercrime Law is informative in showing how the government sought to include broad defamation, sedition and national security-linked offences as potential "cybercrimes", as well as an example of how the law-making process was strongly influenced by other laws in the region – namely *Thailand*'s Cybersecurity Act. In July 2019, it was reported that the Ministries of Justice and Interior were reviewing the draft of the Cybercrime Law.[547] At the time of this publication of this report, it remained unclear as to what exactly the law would regulate or criminalize online as an official draft of the law has not been released for public consultation.

ix. Laws abused to justify internet shutdowns

States in the region face genuine challenges such as proliferation of hate speech and incitement to violence online, online disinformation and threats of cyber-attacks. While the above sections have looked into laws brought into force to purportedly combat online disinformation and protect cybersecurity, this section analyzes how the Telecommunications Law in *Myanmar* has allowed the government to shut down the internet to purportedly ensure public order in response to proliferation of hate speech and incitement to violence online. In addition, this section also addresses *Philippines, Indonesia* and *Vietnam*, where it was not even clear which laws were used to justify police requests to shut down the internet in the interests of ensuring public order. These shutdowns occurred without prior notice to the public and without clear justifications provided by the authorities to explain precise policy and legislative aims behind such measures.

545 *Ibid.*
546 *Ibid.*
547 Mech Dara, 'Ministries review content of draft law on cybercrime', *Phnom Penh Post,* 12 July 2019, Available at: https://www.phnompenhpost.com/national/ministries-review-content-draft-law-cybercrime

As noted, comprehensive internet shutdowns can never be justified under international human rights law. Instances of shutdowns in recent years reflect a real risk that governments in the region may employ this indiscriminate method more often in the future to maintain "public order" through sacrificing the rights to free expression, information, security, assembly association, education, health and work, amongst other rights.

There is already evidence of a growing recourse to the use of shutdowns by governments across the globe. In September 2019, the New York Times reported, referencing research conducted by digital rights organization Access Now, that one quarter of countries in the world had imposed internet shutdowns in the preceding four years, and that they were often imposed during instances of civil unrest or political instability.[548] In a 2018 report, Access Now noted that more than 196 internet shutdowns had been imposed in 25 countries, for reasons of combating disinformation, hate speech, incitement to violence online, national security and public order.[549] In nearly 60 percent of all reported incidents in 2018, State authorities did not acknowledge responsibility for ordering the shutdowns.[550]

Myanmar

As highlighted in the introductory paragraphs to this report, Myanmar faces a severe problem involving proliferation of hate speech online. Indiscriminate and accelerating spread of hate speech and incitement to violence on Facebook was found to have had a role in facilitating gross human rights violations, crimes against humanity and possible genocide of Rohingya Muslims, particularly in Rakhine state. It is within not only this context, but also a wider context of widespread discrimination against members of minority groups throughout the country and continuing strife between different ethnic, racial and religious communities, that the use of internet shutdowns by the Myanmar government should be analysed.[551]

548 NY Times, 2 September 2019.
549 India was responsible for 134 shutdowns, while three shutdowns were recorded in the region – in Indonesia and Philippines – in 2018. See Access Now 2018 report, p 2.
550 Out of the more than 200 incidents of shutdowns reported in 2018, 77 were acknowledged by State entities that had ordered the shutdowns. See Access Now 2018 report, pp. 2, 4, 5.
551 See Section I. The ICJ has also addressed these issues often. See for eg. ICJ, 'Myanmar: scrap 'race and religion laws' that could fuel discrimination and violence', 3 March 2015, Available at: https://www.icj.org/myanmar-scrap-race-and-religion-laws-that-could-fuel-discrimination-and-violence/; ICJ, 'Myanmar: Protection of Rohingya Minority, UN Special Session', 5 December 2017, Available at: https://www.icj.org/myanmar-un-special-session/; ICJ, 'ICJ convenes panel discussion on citizenship and human rights in Myanmar', 24 June 2019, Available at: https://www.icj.org/icj-convenes-panel-discussion-on-citizenship-and-human-rights-in-myanmar/

In Myanmar, section 77 of the **Telecommunications Law** was used to shut down the internet in nine townships in Rakhine and Chin states, amidst intensified armed conflict between the Myanmar military and Arakan Army forces.[552] On 20 June 2019, the Ministry of Transport and Communications issued an order to telecommunications and mobile network providers to shut down access to the internet, noting "disturbances of peace and use of internet activities to coordinate illegal activities" in the regions.[553] Government representatives alleged that the shutdown was necessary for public order and "the benefit of all people", in response to "racial hatred in Rakhine… because of racial hate speech and propaganda on social media".[554]

Section 77 of the Telecommunications Law dictates that the Ministry of Transport and Communications "may, when an emergency situation arises to operate for public interest, direct the licensee to suspend a Telecommunications Service, to intercept, not to operate any specific form of communication, to obtain necessary information and communications, and to temporarily control the Telecommunications Service and Telecommunications Equipments".[555]

Lack of clarity in the provision as to what an "emergency situation" entails, and its failure to include safeguards preventing violations of fundamental rights and freedoms allowed the Myanmar government to impose an internet shutdown in contravention of international human rights law. In its analysis of the government's actions, Article 19 – a non-governmental organization that focuses on freedom of expression – highlighted that the government had not established a legitimate aim for the shutdown, as it had not provided credible or legitimate information on allegations of "disturbances of peace and use of internet activities to coordinate illegal activities" to sufficiently justify a shutdown. It further found that the shutdown had been a disproportionate

552 The townships were Ponnangyun, Kyauktaw, Maungdaw, Buthidaung, Rathedaung, Maruk-U, Minbya and Myebon townships in Rakhine State, and Paletwa township in Chin State. The Arakan Army is an armed group fighting for greater autonomy in Rakhine State. See Free Expression Myanmar, 'Internet Shutdown in Rakhine and Chin States', 24 June 2019, Available at: http://freeexpressionmyanmar.org/internet-shutdown-in-rakhine-and-chin-states/; Myanmar Centre for Responsible Business, 'Lift the Restrictions on Internet Access', 28 June 2019, Available at: https://www.myanmar-responsiblebusiness.org/news/lift-the-restrictions-on-internet-access.html

553 Telenor Group, 'Network shutdown in Myanmar, 21 June 2019', 21 June 2019, Available at: https://www.telenor.com/network-shutdown-in-myanmar-21-june-2019/; Shoon Naing, 'Myanmar orders internet shutdown in conflict-torn Rakhine state: telco operator', *Reuters,* 22 June 2019 ('Reuters, 22 June 2019'), Available at: https://www.reuters.com/article/us-myanmar-rakhine/myanmar-orders-internet-shutdown-in-conflict-torn-rakhine-state-telco-operator-idUSKCN1TN0AX; Telenor Group, 'Update on the network shutdown in Myanmar, 13 August 2019', 13 August 2019, Available at: https://www.telenor.com/update-on-the-network-shutdown-in-myanmar-13-august-2019/

554 Brig. Gen. Zaw Min Tun, a spokesman for the Myanmar military, reportedly stated this, while U Myo Swe, Chief Engineer for Myanmar Posts and Telecommunications, reportedly stated that "The internet will resume when stability is restored" and that the shutdown was "for the benefit of the people". Hannah Beech, Saw Nang, 'The Government Cut Their Internet. Will Abuses Now Remain Hidden?', *New York Times,* 2 July 2019 ('NY Times, 2 July 2019'), Available at: https://www.nytimes.com/2019/07/02/world/asia/internet-shutdown-myanmar-rakhine.html

555 Telecommunications Law, section 77.

measure which breached the government's obligation to employ the least restrictive means to achieve an aim of national security and public order.[556]

Even if the government had provided sufficient national security or public order justifications, however, the blanket shutdown of the internet in Rakhine and Chin states would have still contravened the rights to free expression and information and other rights, including the rights to assembly, association, education, health and work. Humanitarian organizations working in the region reported having difficulties in coordinating humanitarian and relief efforts without internet access, human rights organizations highlighted that monitoring of rights abuses had been crucially restricted, even as armed conflict had intensified during the period of the shutdown, and local lawmakers stated that they were unable to receive updates or information from people in their townships.[557] The UN Special Rapporteur on the human rights situation in Myanmar expressed concern that the shutdown could allow for the military to commit violations against civilians and "do whatever they want under the name of national security".[558] A Member of Parliament from Rakhine State reiterated this concern, stating that the shutdown "destroys the rule of law and security".[559]

As of September 2019, the shutdown had been partially lifted.[560]

Philippines, Vietnam and Indonesia

In the Philippines, Vietnam and Indonesia, legal regulations were not clearly provided for internet shutdowns in the countries – in violation of the requirements of legitimacy, necessity and proportionality for executive measures. While the shutdowns were purportedly advanced to ensure public order, in all the cases below, State authorities failed to provide sufficient evidence, legal justifications or redress or accountability mechanisms to ensure that the fundamental rights and freedoms of individuals would be respected amidst an internet shutdown.

556 Article 19, 'Briefing Paper: Myanmar's Internet Shutdown in Rakhine and Chin States', 2 August 2019, Available at: https://www.article19.org/wp-content/uploads/2019/08/2019.08.01-Myanmar-Internet-Shutdown-briefing-.pdf

557 HRW, 28 June 2019; Reuters, 22 June 2019; NY Times, 2 July 2019; Joint statement on the internet shutdown in Rakhine and Chin States by digital rights organisations and other civil society organisations, *Association for Progressive Communications*, June 2019, Available at: https://www.apc.org/en/pubs/joint-statement-internet-shutdown-rakhine-and-chin-states-digital-rights-organisations-and

558 Al Jazeera, 'US joins calls for Myanmar to end internet shutdown', 30 June 2019, Available at: https://www.aljazeera.com/news/2019/06/joins-calls-myanmar-internet-shutdown-190629181233538.html

559 NY Times, 2 July 2019.

560 Sam Aung Moon, 'Myanmar partially lifts internet shutdown in conflict-torn Rakhine, Chin states', *Reuters,* 1 September 2019, Available at: https://www.reuters.com/article/us-myanmar-rakhine/myanmar-partially-lifts-internet-shutdown-in-conflict-torn-rakhine-chin-states-idUSKCN1VM13J

In *Philippines*, in January 2015, telecommunications providers shut down mobile services and internet connections during a five-day visit of Pope Francis, pursuant to directions from the National Telecommunications Commission (NTC).[561] The shutdown was justified on the basis of the need to ensure the safety of the Pope as mobile devices could be used to trigger explosives.[562] In January 2018, Filipino media-monitoring group Foundation for Media Alternatives (FMA) expressed concern that "shutting down communication networks is becoming the norm", noting 11 instances of shutdowns between 2016 and 2017 that the NTC had approved, namely during the Sinulog, Dinagyang and Feast of the Black Nazarene festivals.[563] FMA called for transparency in shutdown implementation procedures to guard against potential abuse by the authorities, emphasizing that "(s)tripping the general public of their means to communicate restricts them from contacting emergency services, authorities, and each other; paralyzes their businesses and jobs; and further places them at risk".[564]

In *Vietnam*, in May 2016, the government shut down access to Facebook during a three-day visit of then-US President Barack Obama in an apparent attempt to silence activists, human rights defenders or dissidents, who often use the social media platform for advocacy. Access Now criticized the Vietnamese government's move, stating, "in the name of public safety, shutdowns instead cut off access to vital information, e-financing, and emergency services, plunging whole societies into fear and destabilizing the internet's power to support small business livelihoods and drive economic development."[565] Access to Facebook had been restricted or blocked in other instances earlier in that same month, ahead of parliamentary elections and during a period where protests had intensified in response to an environmental disaster.[566]

561 Lynda C. Corpus, 'Papal visit: Netizens react to disrupted telco services', *Rappler,* 16 January 2015, Available at: https://www.rappler.com/specials/pope-francis-ph/81044-netizens-react-disrupted-telco-services-papal-visit

562 Mick Basa, 'No network service? It's for Pope's safety, say telcos', *Rappler,* 16 January 2015, Available at: https://www.rappler.com/specials/pope-francis-ph/80989-telcos-disrupt-signal-pope-visit; Rappler, 'As Pope Francis leaves, network services returns to normal', 19 January 2015, Available at: https://www.rappler.com/specials/pope-francis-ph/81369-pope-francis-leaves-network-signals-back-normal

563 Interaksyon, 'Internet shutdowns: A myth of security and public safety', 26 January 2018, Available at: http://www.interaksyon.com/infotek/2018/01/26/117929/internet-shutdowns-a-myth-of-security-and-public-safety/

564 *Ibid.*

565 Access Now, 'Vietnam blocks Facebook and cracks down on human rights activists during Obama visit', 23 May 2016, Available at: https://www.accessnow.org/vietnam-blocks-facebook-human-rights-obama/

566 Yasmeen Abutaleb, 'Vietnam restricted access to Facebook during Obama visit: activists', *Reuters,* 27 May 2016, Available at: https://www.reuters.com/article/us-vietnam-obama-facebook-idUSKCN0YH2MZ

In *Indonesia*, in May 2019, the government introduced restrictions on uploading videos, voice messages and images on social media platforms such as Twitter, Facebook, WhatsApp and Instagram, following the eruption of riots in Jakarta after national election results were released, where hundreds of people had been injured and some killed.[567] The restrictions were justified on the basis of preventing disinformation and hoaxes exacerbating racist sentiments and religious tensions that had spread quickly and widely after the riots – Coordinating Minister for Political, Legal and Security Affairs Wiranto noted that they would "avoid provocations and the spread of fake news through the community" while Minister of Communications and Information Technology Rudiantara stated that restrictions would reduce circulation of imagery which could "inflame" emotions.[568] The Ministry of Communications and Information Technology further warned members of the public that circulating content inciting violence or hatred were offences under the UU ITE.[569]

Even as the UU ITE provides authorities with the power to control the spread of disinformation online, civil society and academic observers in Indonesia expressed concern that the restrictions on social media had been imposed arbitrarily and in contravention of rule of law, as the government had neither explicitly cited the UU ITE, nor any other decree or legal justification, for the restrictions.[570] In addition, the government had reportedly failed to specifically point out "indicators" leading to the access restrictions.[571] A lack of transparency regarding the government's scope of control over the internet also raises other serious concerns about State surveillance of social media platforms and data security. Commentators have recommended that more resources invested instead into strengthening data literacy in the country.[572]

567 Netblocks, 'Indonesia blocks social media as election protests escalate', 22 May 2019, Available at: https://netblocks.org/reports/indonesia-blocks-social-media-as-election-protests-escalate-XADE7LBg; Trisha Jalan, 'Update: Indonesia lifts social media restriction after 3 days', *Media Nama,* 27 May 2019, Available at: https://www.medianama.com/2019/05/223-indonesia-restricts-social-media/

568 *Ibid.*; Coconuts Jakarta, 'Police deny entering mosques in pursuit of rioters as hoaxes about secret Chinese soldiers go viral', 22 May 2019, Available at: https://coconuts.co/jakarta/news/police-deny-entering-mosques-in-pursuit-of-rioters-as-hoaxes-about-secret-chinese-soldiers-go-viral/

569 Karina Tehusijarana, Jessicha Valentina, 'Jakarta riot: Government temporarily limits access to social media, messaging apps', *Jakarta Post,* 22 May 2019, Available at: https://www.thejakartapost.com/life/2019/05/22/jakarta-riot-government-temporarily-limits-access-to-social-media-messaging-apps.html?src=mostviewed&pg=/

570 Resty Woro Yuniar, 'Indonesia's listening in on private internet chat groups. WhatsApp with that?', South China Morning Post, 24 June 2019 ('SCMP, 24 June 2019'), Available at: https://www.scmp.com/week-asia/economics/article/3015612/indonesias-listening-private-internet-chat-groups-whatsapp

571 SCMP, 24 June 2019. Observers also highlighted that one week before the riots had broken out, Whatsapp had reportedly removed 61,000 users in compliance with a request from Rudiantara on the basis that the users had "broken rules" – Legal basis had also not been provided by the authorities.

572 SCMP, 24 June 2019.

IV. Patterns of abuse

While the laws and their implementation as outlined in this report reflect particular legal systems and must be understood in their national contexts, a number of important commonalities emerge, revealing a pattern of abuse across the region. In many instances, the legal provisions themselves are not human rights compliant, and these deficiencies are exacerbated by the manner in which they have been implemented. Legal frameworks have thus been abused systematically to curtail the exercise of the rights to freedom of expression, opinion and information, and other human rights and fundamental freedoms, online.

i. "National security" and "public order"

The first commonality is that the laws covered in this report often conflate national security, public order and related themes with the perceived interests of the government or other powerful actors. There is often further conflation with protection against offence or insult to the reputation or dignity of individual representatives of the State – including State officials, the head of State or the monarch, or organs of the State, including the judiciary. The laws and regulations are riddled with vague, imprecise language, in contravention of the principle of legality. This leaves them open to arbitrary application across a wide range of circumstances, with substantial discretion given to officials with little accountability.

In many of the cases referenced in this report, individuals have been detained, investigated, charged, prosecuted and/or convicted of offences, even where a specific, narrow link between the act of online expression of an individual and its "real, identifiable risk of significant harm" to a "legitimate security interest" has not been shown,[573] or where the information they revealed online should be protected expression because they concern matters of "public debate concerning public figures in the political domain and public institutions".[574]

It is clear from the classes of individuals and legal persons who have been targeted that laws have been misused to control political and other critical debate online in order to protect the interests of powerful individuals or institutions. Those targeted with prosecution had all expressed or revealed

573 Tshwane Principle 3.
574 CCPR/C/GC/34, para 38.

information deemed unfavourable to the ruling government of the State, or been associated with political opposition. Some individuals have been subject to legal harassment by companies for bringing to light human rights violations, without sufficient protections provided by the State to ensure that they can carry out their research, advocacy or reporting independently and safely – in contravention of the UNGPs.

This report has highlighted specific cases which reflect the politically-motivated nature of these prosecutions and how "national security" has often been conflated with protecting the ruling government from criticism. The sedition cases brought against **Zunar**, **Eric Paulsen** and **S. Arutchelvan** reflected how severe charges were dropped soon after the change of a government in ***Malaysia*.** Similar sedition-linked charges launched against **Vice President Leni Robredo** and officials of the opposition Liberal Party in the ***Philippines*** soon after the 2019 general elections also appeared to have been undertaken for political reasons, targeting not only the party, but also members of the clergy and lawyers who had expressed dissent against the conduct of President Duterte. Meanwhile, the case of **Jakarta Globe**, **Okezone** and **Harian Bangsa** showed a spuriousness in decision-making when the police in ***Indonesia*** were able to drop alleged defamation charges very quickly after they were brought against the news outlets and its journalists. In ***Thailand,*** lesè majesté and sedition cases were tried in military courts as they purportedly related to "national security" only after the military-led government came into power; while in ***Cambodia,*** the coming into force of the inter-ministerial *prakas* just before the 2018 elections and the shutdown afterwards of news websites days before the elections reflected the fact that the government had brought the law into force to censor independent reporting surrounding the elections. In ***Malaysia***, the **Sarawak Report** was similarly blocked through the CMA by a government seeking to contain spread of information regarding the 1MDB scandal when that information was most necessary in the public interest of the Malaysian people.

"National security" and "public order" have also been used as pretextual justifications for full or partial shutdowns of the internet in *Myanmar, Philippines, Vietnam* and *Indonesia* – often without providing any legal basis at all. This impedes a range of rights, including freedoms of expression, assembly and association, and the rights to information, education, health and work. While there are real security concerns relating to the spread of disinformation, hate speech and incitement to violence, governments have

generally failed to provide clear legal justifications which assessed the legality, proportionality or necessity of a shutdown against these concerns, in line with their obligations to protect human rights. The shutdowns exacerbated, rather than ameliorated, safety and security concerns of the public, and in *Myanmar* and *Vietnam*, potentially facilitated the commission of more human rights violations by removing internet access from rights monitoring groups, human rights defenders and activists. In *Myanmar*, in particular, the shutdown had the effect of preventing documentation and information about human rights violations from being reported.

ii. Vague, overbroad provisions

The second commonality between the laws is that they have vague, overbroad provisions which confer wide, overbroad powers on State authorities and allow implementation of the laws to be dictated by the inclinations of the person or authority body enforcing such laws, thus preventing individuals – and indeed government officials themselves and the judiciary – from being able to discern clearly which kinds of expression or information might be subject to restrictions.

Thus, ***Myanmar*'s Telecommunications Law**, which was brought into force to "enable the supervision" of telecommunications services, network facilities and equipment "for national peace and tranquility and for public security", does not define clearly what "national peace and tranquility" entails, and on their face, these categories are not legitimate bases for restricting rights.[575] Section 77 of the law also fails to set out preconditions to determine an "emergency situation" – allowing for authorities to be able to impose blanket internet shutdowns on entire regions of the country. Similarly ***Thailand*'s Computer-related Crimes Act** offers no clear direction on acts "likely to cause damage to the protection of national security, public safety… or cause panic to the public".[576] Overbroad provisions which do not clarify what raising "unrest" or "disaffection" mean have been highlighted in the sedition laws of ***Thailand, Myanmar, Malaysia***, ***Brunei*** and ***Philippines***, and "propaganda against the state", "causing disorder", "disruption of security" and "being useful to an enemy" are terms left vaguely defined in the laws of ***Laos, Vietnam*** and ***Myanmar*** to cover a wide range of acts, including legitimate expression of opinion, that can fall under espionage-like

575 Myanmar Penal Code, section 4(e).
576 See Section III (i).

offences.[577]

Newer laws suffer from the same limitation of vague, overbroad provisions. ***Singapore's*** **AJPA** lowers the threshold for scandalizing the judiciary to mere "risk" of undermining public confidence in the judiciary, when the common law threshold of "real risk" had already shown to be wide enough to allow for persecution of individuals expressing disfavoured views, while its **POFMA** allows for nearly any form of communication – written, visual, audio or otherwise – to be targeted and classified as a criminally liable "false statement of fact". The ***Philippines'*** **AFC Bill** similarly includes overbroad definitions of "fake news", without setting out clear tests for what constitute "false" or "misleading" information – as did ***Malaysia's*** **AFNA** before its repeal. This absence of guiding principles prevents people – including the authorities themselves - from being able to ascertain with certainty what information is or is not criminally liable. Meanwhile, ***Vietnam's*** **LOCS** and ***Thailand's*** **Cybersecurity Act** fail to clarify that "national security" and "public order" must be interpreted to include protections for fundamental rights and freedoms and leave these terms vague and open to wide interpretation – even when these justifications underpin the entire framework and implementation of cybersecurity measures detailed under the laws. These laws, again, allow for and facilitate executive overreach.

iii. Severe penalties

A third commonality that is clear is that penalties provided for under the laws are neither necessary nor proportionate towards their purported objectives, reflecting a targeted, punitive intent to penalize and silence critical dissent.

Defamation is criminalized in ***Thailand, Myanmar, Indonesia, Singapore*** and ***Philippines***, in contravention of international human rights law and standards. Thus, crucially, the UN Human Rights Committee clarified in the case of **Alexander Adonis** that the *Philippines* had violated the ICCPR in imposing criminal sanctions against the journalist, and noted that Philippines was "under an obligation to take steps to prevent similar violations occurring in the future, including by reviewing the relevant libel legislation".[578] The Philippine government, however, did not take such preventive steps and in fact worsened the capacity of its domestic laws to

577 See Section IV (iv).
578 CCPR/C/103/D/1815/2008, para 10.

commit such violations, by introducing the **Cybercrime Prevention Act** that expanded criminalization of defamation to the online sphere, increasing penalties for alleged "cyberlibel".

Excessive penalties imposed upon individuals highlight the sheer severity and lack of proportionality in legal sanctions imposed by governments against perceived dissent in the region. A ***Vietnamese*** activist who sought to raise awareness of environmental issues was sentenced to life imprisonment. ***Thai*** individuals were tried for posting comments on Facebook deemed "insulting" against the monarchy and given 35-year, 30-year and 28-year imprisonment terms – which were themselves halved from original 70-year, 60-year and 56-year sentences because the defendants had pled guilty. A ***Malaysian*** cartoonist faced potentially 43 years in prison for political satire. ***Laotians*** who had made critical comments on Facebook against their government while in Thailand were imprisoned for 12 years, 16 years and 20 years and made to pay fines between 110 million to 210 million kip. This amounted to approximately USD 12,000 to USD 24,000, a fine that is exorbitant even in countries where the State's GDP per capita or the daily wage of an individual are far higher. The Thai military sought 10 million Baht (approx. USD 330,000) in damages against a ***Thai*** news website for news reporting. A ***Singaporean*** blogger was made to pay S$150,000 (approx. USD 110,000) to the Prime Minister for alleged defamation A ***Bruneian*** government employee fled after facing potential fines of up to B$16,000 (approx. USD 12,000) for making a comment criticizing a government policy. News platforms were unilaterally blocked in ***Malaysia*** and ***Cambodia*** for merely engaging in professional journalistic reporting, and **Rappler** in the ***Philippines*** is currently facing 11 separate legal actions for independent journalism – incurring also hefty costs in legal fees. Entire townships in ***Myanmar*** were deprived of internet access, during a period of armed conflict when such access was even more crucial for communication with family, friends, townspeople and to access health, social or emergency services.

Newer legal regulations – under ***Singapore's*** **POFMA**, ***Laos'*** **government order** to register social media platforms, ***Vietnam's*** **LOCS** and ***Thailand's*** **Cybersecurity Act** – also problematically sanction severe penalties in imprisonment terms and hefty fines which are not countenanced by provisions ensuring adequate and independent oversight and accountability mechanisms.

iv. Lack of independent oversight mechanisms

The fact that – and ease with which – State authorities have systematically misused laws in the region highlights the fourth commonality. These laws do not provide for independent oversight mechanisms to safeguard against their misuse.

In the ***Indonesian*** case of **Anindya Joediono**, the investigation of her alleged criminal defamation under the UU ITE was conducted by the police, even though the alleged defamatory comment had accused police officers of sexual assault. In ***Thailand***, military courts have been used to conduct the trials of civilians, violating their most basic rights to fair trial, let alone providing them with recourse to review by an independent mechanism. (It is hoped that a recent order by the Prime Minister will now phase out this practice.) In ***Singapore***, the **Administration of Justice (Protection) Act** dictates to independent judicial bodies the criminal extent of the offence of contempt of court, despite judicial pronouncements under common law which have neither reflected nor called for the severity of penalties proposed under the Act. In ***Malaysia*** and the ***Philippines***, the **Communications and Multimedia Act** and the **Cybercrime Prevention Act** did not empower independent mechanisms with mandates to impartially review decisions of the MCMC and the DOJ where they were in violation of fundamental rights and freedoms, as was the case with **Sarawak Report, Medium, The Malaysian Insider, Maria Ressa** and **Reynaldo Santos Jr**. Meanwhile, within the laws of ***Laos*** and ***Vietnam***, executive, legislative and judicial powers are so explicitly intertwined and controlled by the Lao Peoples' Revolutionary Party and the Communist Party of Vietnam that an independent oversight mechanism is near impossible.

Independent oversight mechanisms would be best placed to determine cases of complaints filed by individuals or legal persons against individual representatives of the State or government authorities that breach the same laws. Currently, most of the laws covered in this paper do not even include legal provisions allowing for complaints to be filed by defendants against State representatives or bodies. In most of the cases, charges were mounted against individuals and legal persons by prosecutors, police, the military or other authorities linked to the State and also business enterprises, while targeted individuals had no judicial, administrative or other avenue to seek independent assessment of their claims of defence.

The independence of the judiciary is also an important consideration in assessing the effectiveness of oversight mechanisms. Such an assessment must also consider the scope of judicial power granted to the courts under domestic laws, including whether and how the laws criminalize speech which should not be criminalized and allow for executive overreach and large financial penalties. Legal systems must allow not only for judicial review of regulatory bodies in specific individual cases, but for review of a law itself, such as was the case in the ***Philippines***' Supreme Court's review of the **Cybercrime Prevention Act**.

The cases highlighted in this report suggest that the judiciary cannot always be relied upon as a sole oversight mechanism – particularly in countries where the judiciary is not independent. Meanwhile, even where the judiciary functions independently, the emergence of contemporary laws and regulations that apply specifically to online platforms increasingly require input, analysis and assessment by not only independent individuals with technical ICT expertise, but also academics, lawyers and members of civil society who can integrate a human rights-centred approach in reviewing cases which are brought under these new "offences". Independent and impartial oversight mechanisms should be put in place to safeguard against infringements on the rights to freedom of expression and information online.

v. Failure to provide effective remedy or accountability

The fifth commonality – exacerbated by executive overreach and the absence of independent oversight mechanisms – is the absence of legal provisions for effective remedy, including judicial remedy, or accountability – which in turn explains how severe penalties were imposed on individuals in the first place.

The right to effective remedy includes the need for adequate and effective legislative, administrative or other appropriate mechanisms to be incorporated within the provisions of a law to prevent violations of the rights to freedom of expression and information, and specific legal provisions guaranteeing prompt and effective remedies or reparation, including compensation, satisfaction, restitution and/or guarantees of non-repetition, should a court of law find that an individual's rights were violated.[579]

579 ICJ, 'The Right to a Remedy and Reparation for Gross Human Rights Violations: A Practitioners' Guide, Revised Edition 2018', pp. 53, 54.

With respect to defamation and *lèse majesté* laws, criminal penalties should be removed entirely, and the defences of truth and fair comment – which protects the publication of information deemed in the interests of the public – must be provided for in the civil legal regimes governing these acts. Laws should also provide that they cannot be applied to punish untrue statements which were published in error but not with malice, and were shown to be in the interests of the public.[580] The defence of "innocent dissemination" is also crucial with respect to the spread of information online – to protect "secondary" publishers who can show that they had "no actual knowledge" of an alleged offence, were not cognizant of any "circumstances to put them on notice" of an alleged offence, and "committed no negligence in failing to find out" about the offence.[581]

These defences should also apply in cases relating to national security, sedition and contempt of court, and cases which fall under laws regulating online information which extend criminalization of these offences to the online sphere. With respect to contempt of court, the defence of "innocent dissemination" also applies to protect information relating to a court case which was disseminated by a person, a journalist for example, who was unaware that the court case was still active at the time of dissemination.[582]

As offences of "spreading disinformation online" and "compromising cybersecurity" are relatively new, assessment of suitable and effective redress and accountability mechanisms for individuals alleged to have committed such offences would be well served by the establishment of independent and impartial committees – staffed with individuals who have ICT expertise as well as lawyers, academics and civil society who can assist in providing a human rights framing and analysis. Independent and impartial commissions could be proposed as a mechanism to assess and review executive or judicial decisions made under the new laws, and advise on the development of the legal framework itself. The defences of truth, fair comment and "innocent dissemination" can also be expanded to apply to individuals accused of "spreading disinformation online" or "compromising cybersecurity". These commissions could interact with other regional or international mechanisms

580 CCPR/C/GC/34, para 47.

581 David Potts, 'Defence of Innocent Dissemination at Common Law', Available at: http://www.cyberlibel.com/?page_id=761; Referring *to Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, SCC 45 (CanLII) [2004] 2 S.C.R. 427 at [89].

582 See UK's Law Commission clarifying this defence in the context of contempt of court cases in its 'Law Commission Consultation Paper No 209: Contempt of court – Summary for non-specialists', Available at: http://www.lawcom.gov.uk/app/uploads/2015/03/cp209_contempt_of_court_summary.pdf

tasked with dealing with these contemporary problems, and integrate national, regional and international perspectives on tackling these globally relevant challenges and establishing effective remedy and accountability mechanisms.

vi. Application beyond frontiers

The sixth commonality evident from the legal frameworks covered in this report is the attempt to reach beyond national frontiers. Laws which had in previous decades been promulgated, interpreted and applied to written or spoken expression or published writing or imagery within a country, have been increasingly applied to information which originates from outside a State's territory. These laws have also been sought to break down the distinction between public and private, communications – by conflating expression on publicly accessible and private (including encrypted) platforms.

International human rights law is clear that States' obligations under the international framework extend not only within their territory but also extraterritorially – States have obligations to respect, protect and fulfil human rights, including civil, cultural, economic, political and social rights, in situations over which they exercise authority or effective control, whether or not such control is exercised in accordance with international law, as well as in situations over which State acts or omissions bring about foreseeable effects on the enjoyment of human rights, whether within or outside its territory.[583]

Extraterritorial application

Though only some laws like ***Singapore's*** **POFMA** and ***Vietnam's*** **LOCS** explicitly provide for extraterritorial application, the other laws covered in this report also engage concerns about extraterritorial impacts on individuals who are not physically within a national jurisdiction. Given the global nature of the internet, censorship within a certain jurisdiction necessarily engages the rights to freedom of expression or information of individuals situated outside of that territory, who seek access to such information. This is especially evident with respect to online news websites – which are not only read by people within a country – and where access

583 This was affirmed by the UN Human Rights Committee in its General Comment No. 31, the Maastricht Principles on Extraterritorial Obligations of States (see footnote 83), and the UN High Commissioner of Human Rights in his 2014 report on the right to privacy (see footnote 52). See also ICJ, 'Protecting Human Rights Beyond Borders', 25 November 2012, Available at: https://www.icj.org/protecting-human-rights-beyond-borders/; UN Human Rights Committee, 'General Comment No. 31 - The Nature of the General Legal Obligation Imposed on States Parties to the Covenant', 26 May 2004, CCPR/C/21/Rev.1/Add. 13.

to the internet is shut down.

In the case of **Manager Online**, for example, criminal defamation charges led to a settlement where the news website was compelled to publish a "clarification statement" on its website. These could have negatively impacted upon the rights of academics, researchers or civil society representatives who reside outside of ***Thailand*** to receive accurate information regarding a case of torture or ill-treatment within the country. Similarly, in ***Myanmar***, the internet shutdown in Rakhine and Chin states restricted access to information by individuals and lawmakers within townships as well as access by those working with humanitarian and human rights organizations who required such information to deliver necessary services.

Extraterritorial reach not only increases risks of infringing the rights of individuals but also places obstacles and onerous requirements on authorities or corporate bodies in other jurisdictions that are implementing their obligations to protect free expression, opinion and information. Thus, ***Singapore's*** **POFMA**, places burdens on internet access providers and internet intermediaries to limit any expression or information deemed in violation of the law as long as the end-user is situated in Singapore. These burdens are likely to not only impact ICT companies but also journalistic outlets. International news organizations have been subject to defamation proceedings and slapped with excessive fines for reporting on matters deemed to violate the law in Singapore. ***Vietnam's*** **LOCS**, meanwhile, not only increases risks of infringement of the right to privacy of individuals through data localization in Vietnam but also places burdens on ICT companies to remove information from their platforms, which can impact on the rights of users of the platforms outside of Vietnam. States have the right to regulate ICT companies to ensure protections against rights violations online, but these regulations should not be drafted, interpreted or enforced in a manner which facilitates or enables rights violations.

Information intended to be public vs. information intended to be private

Previously clear distinctions between private and public communications have also been complicated by some of these legal frameworks. Posts or information shared on Facebook on "public" settings, for example, can be generally deemed to have been shared with an intention to make them public information,[584] while messages shared between individuals via Whatsapp

584 Facebook, 'What is public information on Facebook?', Available at: https://www.facebook.com/

are generally intended to be private. Such privacy interests were reflected by end-to-end encryption built into the application by its makers.[585] This report notes that there are existing, pertinent questions about whether ICT companies adequately protect the right to privacy of its users. However, it can be generally accepted that messages sent in an encrypted service to a particular individual as opposed to posts put on a platform for public viewing reflect different intentions on the part of the originator of such information.[586]

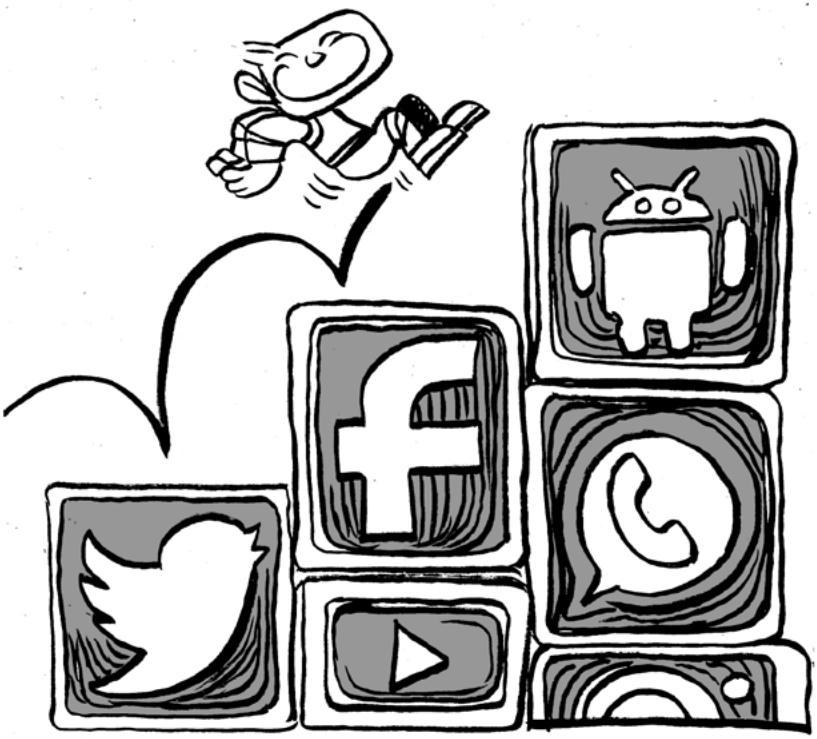
Cases emerging in the region show that governments appear to be willing to apply laws, that are already non-human rights compliant on their face, not only to expression or information shared on an online platform for public viewing, but also to content intended to be private by the person who drafted or disseminated it. In ***Brunei***, a woman was detained and questioned by the police for Whatsapp messages criticizing the police, while in ***Malaysia***, a man was detained for three days following a message he had sent via Whatsapp which was deemed insulting to former Prime Minister Najib Razak. In ***Singapore***, **Li Shengwu** is facing contempt of court proceedings for a Facebook post he had made on a "Friends Only" privacy setting – which can be construed to have been meant to limit the information to a selected number of people.

This concern is pertinent with respect to measures such as data localization under ***Vietnam's*** **LOCS** and provisions under ***Thailand's*** **Cybersecurity Act** which allow for State authorities to enter premises, search and seize electronic data and equipment from any legal person, make copies of such data, test electronic equipment or systems and request "real-time" access to information held by private entities also raise concerns about increased intrusions of privacy for a purported aim of maintaining "national security" or "public order", which may not be legitimately defined or proportionately enforced.

help/203805466323736

585 End-to-end encryption ensures information is retained between two users in a conversation, through measures which ensure each message sent has a "unique lock and key" that increases security. See Whatsapp, 'Whatsapp Security', Available at: https://www.whatsapp.com/security/

586 See, on ICT companies and the right to privacy of users, Amnesty International, 'Surveillance Giants: How The Business Model Of Google And Facebook Threatens Human Rights', November 2019, Available at: https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF



V. Moving forward

Laws, regulations, policies and practices continue to be designed in non-human rights compliant ways by States in Southeast Asia, and interpreted and applied to unduly restrict the rights to freedom of expression, opinion and information online. There is therefore a crucial need for States to implement international law and standards and give full effect to their human rights obligations regarding these rights. International human rights law and standards provide the most compelling framework within which to inform and substantiate the efforts of States to protect, respect and fulfil human rights online as they seek to address other emerging law and policy issues. The UN Special Rapporteur on freedom of expression unequivocally clarified in 2011 that the ICCPR had been drafted with "foresight to include and to accommodate future technological developments" for persons to exercise their rights "through any media" and "regardless of frontiers".[587] At least for the suite of laws addressed in this report, and their application, the ICJ holds that this statement holds true.

The UNGPs are also crucially relevant with respect to States' obligations to protect and promote human rights online, given the need for States to integrate obligations and demands on ICT companies to enable and give effect to physical limitations on free expression and information on online platforms. In a 2018 report, the UN Special Rapporteur on freedom of expression raised concerns regarding this co-dependence of the State and the corporate in content regulation online, which are just as relevant to Southeast Asia as to the rest of the world:

"Broadly worded restrictive laws on "extremism", blasphemy, defamation, "offensive" speech, "false news" and "propaganda" often serve as pretexts for demanding that companies suppress legitimate discourse. Increasingly, States target content specifically on online platforms. … Many States also deploy tools of disinformation and propaganda to limit the accessibility and trustworthiness of independent media. … Some States impose obligations on companies to restrict content under vague or complex legal criteria without prior judicial review and with the threat of harsh penalties.

(S)uch rules involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a

587 See Section II (v).

broad effort to avoid liability. They also involve the delegation of regulatory functions to private actors that lack basic tools of accountability. Demands for quick, automatic removals risk new forms of prior restraint that already threaten creative endeavours in the context of copyright. Complex questions of fact and law should generally be adjudicated by public institutions, not private actors whose current processes may be inconsistent with due process standards and whose motives are principally economic".[588]

The UN Special Rapporteur thereafter provided recommendations to States to guide their efforts to protect the rights to free expression, opinion and information online within the contemporary context of a digital age.[589] The following recommendations to governments in Southeast Asia are guided by the Special Rapporteur's formulation:

a) States should repeal any law, regulation or legal framework that criminalizes or unduly restricts expression, online or offline – or take necessary steps to amend or otherwise rectify such laws, regulations or legal frameworks to bring them in line with their international legal obligations;

b) States should repeal any law, regulation or legal framework criminalizing defamation, in line with their international legal obligations;

c) States should refrain from adopting legal frameworks or regulatory models, and amend existing frameworks or regulatory models, where State authorities or agencies, rather than judicial authorities, are arbiters of lawful expression;

d) States should refrain from adopting legal frameworks or regulatory models, and amend existing frameworks or regulatory models, which delegate responsibility to companies as adjudicators of content, which empowers corporate judgment over human rights values to the detriment of users;

e) States should only seek to restrict content online pursuant to an order by an independent and impartial judicial authority and in accordance with due process and the standards of legality, necessity and legitimacy. Existing legal frameworks or regulatory models governing content regulation online should be accordingly amended.

588 A/HRC/38/35, paras 13, 15.
589 A/HRC/38/35, para 64.

Tightly targeted regulation, not heavy-handed viewpoint-based regulation, should be relied upon, focused on ensuring company transparency and remediation to enable the public to make choices about how and whether to engage in online fora;

f) States should refrain from imposing disproportionate penalties, such as excessive fines or imprisonment terms, on individuals, internet intermediaries or internet service providers, through content regulation laws or regulations, given their significant chilling effect on free expression online;

g) States should refrain from establishing laws, legal frameworks or regulatory models which enable "proactive" monitoring or filtering of content online, which can infringe upon the right to privacy and likely facilitate pre-publication censorship;

h) States should publicly publish detailed transparency reports on all content-related requests issued to individuals, internet intermediaries and internet service providers, and involve genuine inputs from the public – including civil society, academics, lawyers, ICT experts and other independent policy advisers or technical experts – in all considerations of appropriate legal frameworks or regulatory models;[590]

i) States should refrain from comprehensively shutting down the internet. In exceptional circumstances, where they restrict – in a narrow, proportionate and limited manner – access to the internet or online services for a legitimate aim, they should clearly and publicly provide justifications for such limitations and alternative measures for access that will uphold the rights of individuals to free expression, information, security, assembly association, education, health and work, amongst other rights.

These recommendations will also assist, and should be undertaken along with, efforts taken by States and ICT companies to respect the right to privacy online, which is also crucially affected when laws, regulations or legal frameworks enable undue restrictions of the rights to free expression, opinion, privacy and information online.

590 (a) to (g) are drawn from the Rapporteur's report, see A/HRC/38/35, paras 65 to 69.

VI. Conclusion

For nearly all forms of private and public expression, including on issues of public interest essential to the functioning of democracy, the internet is increasingly the primary venue for communication, debate and discussion. Distinctions between communications conducted online or offline, in private and or in public, are becoming ever narrower.

Legal and regulatory frameworks designed to protect rights are struggling to take into account more contemporary challenges posed by cyberspace, where the frontiers of ethics, law, business and technology – and where they interact and collide – remain in a state of flux and constant evolution. However, core human rights principles, legal obligations and other standards, which remain applicable online as well as offline, should remain the point of departure. Whatever the gaps in laws regulating new technologies, many of the cases and situations highlighted in this report would be conducive to resolution simply by good faith implementation of well settled international human rights law.

This report has thus sought to identify one starting point for a more comprehensive and forward-looking conversation about how international human rights law can help frame the development and implementation of legal frameworks affecting expression, information-sharing and political participation in the era of the internet.

Concerns surrounding the spread of false information, hate speech and incitement to violence online or cyber-attacks are serious problems that demand solutions. These contemporary problems require urgent and effective action – but action that also protects the rights of individuals, including their rights to life, security, bodily integrity and privacy. Blunt, bad-faith legislative attempts by governments to combat these challenges such as those documented in this report are likely to be ineffective, socially disruptive and costly, if they do not take into account the impacts on human rights and fundamental freedoms.

As technologies of surveillance and control further develop, including artificial intelligence and automation of surveillance technologies, governments will be tempted to exercise even greater control when such control suits its purposes. Without adequate attention to the impacts of these technologies, and with outdated legal and regulatory frameworks and mechanisms at the national and international levels, there is a real danger that the types of violations documented in this report will become more and more common.

This makes it imperative that we ensure that human rights principles and tools are taken into account now.

There are a few final points worth making in this regard.

First, the internet has enabled unprecedented flows of information at the global level such that domestic laws infringing on free expression or information in one country necessarily affect the rights of individuals elsewhere. Decisions and technologies affect people across borders, such as when a person in Rakhine State in Myanmar cannot communicate with a relative in Malaysia in the midst of an internet shutdown, or when a journalist based in Estonia is charged for releasing an article deemed "prejudicial to the security of Singapore". Meanwhile, strict regulation of information online in one country or data localization requirements in another could expose individuals to legal vulnerabilities or physical violence for speech made in an entirely different national jurisdiction.

Secondly, the internet has enabled vast data collection and preservation, which has made exploiting information easier by providing sheer amounts of data to authorities trained in data analytics techniques. 'Likes' or 'shares' on social media platforms now disseminate content with much more rapidity than distributing or disseminating newsletters deemed "prejudicial to the State". Online platforms can now, for example, circulate a video deemed "insulting to the King" through multiple fora within minutes without even the owner of the platform knowing or realizing. While big data has the potential to fuel positive strides forward in development of technologies to enhance human living – through improving communications, health, education or transport for example – it can also be manipulated or misused by States to surveil, control and violate the rights of individuals.

Thirdly, legal frameworks enabling control and regulation of the internet covered in this paper all operate to create an unequal playing field between governments and individuals. Individuals can be targeted and controlled online and deprived of internet access, while governments are free to release any information online, false or otherwise, and do with individuals' data whatever they deem "necessary" or "appropriate" under the guise of "national security" or "public order". An ordinary individual has few resources to ascertain or even understand the full extent of the information available about them online, and can be easily targeted for something said or posted years prior. An internet shutdown is the most extreme example of this imbalance of power over data and information.

Finally, the internet today has emerged as the primary arena in which States today contend with global companies, particularly big technological companies, for political influence, power and control – gradually edging out the voices and concerns of individuals in the process. States' obligations to protect security today no longer fall purely under the authority of the State, and increasingly require collaboration with and limitations on the operations of big technological companies to give effect to the State's aims. In 2017, the government of Denmark became the first country in the world to post an Ambassador to the tech industry, in an attempt to represent the nation's interests at Silicon Valley and influence the effects of technology on its society. As Ambassador Casper Kynge, observed, "(o)ur values, our institutions, democracy, human rights … are being challenged right now because of the emergence of new technologies … These companies have moved from being companies with commercial interests to actually becoming de facto foreign policy actors." Within this contemporary dynamic, rights are at risk of erosion not only by States but also by companies operating on a global level.

The protection of human rights in the 21st century requires the development of international legal and regulatory frameworks which must involve States in full consultation with the UN and other, international authorities, along with legal, human rights and ICT experts. This will best be achieved with the engagement of technological companies who operate on a global level. Protection of human rights online is required not only for freedom of expression and information to be protected online but also for protection of rights against threats posed by the spread of hate speech, incitement to violence and disinformation online, cyber-attacks and other cybercrimes.

The international human rights framework governing freedom of expression and information remains crucially relevant today and provides more than sufficient guidance with respect to the legal frameworks covered in this report and their misuse by governments in Southeast Asia to clamp down on the fundamental freedoms of individuals. These legal frameworks have been shown to be less than fit for purpose in various ways, and do not advance legitimate aims in accordance with the principles of legitimacy, necessity and proportionality required by the rule of law. They should be repealed, amended or otherwise rectified to be brought in line with international human rights principles governing freedom of expression, opinion and information, towards fulfilling States' obligations under international human rights law.

VII. Annex

Laws, regulations and bills referenced in this report included:

(In order of appearance in report)

Brunei Darussalam	❖ Sedition Act 1948 ❖ Internal Security Act 1982 ❖ Telecommunications Act 1974
Cambodia	❖ Criminal Code ❖ Inter-ministerial order (prakas) of 2018 adopted by the Ministry of Information, Ministry of Interior and Ministry of Posts and Telecommunication ❖ Draft Cybercrime Law (not in force)
Indonesia	❖ Penal Code ❖ Law on Electronic Information and Transactions 2008
Lao PDR	❖ Criminal Code ❖ Decree No. 327 On Information Management on the Internet ❖ Government order "controlling the spread of fake news and disinformation on social media" (2019) ❖ Law on Prevention and Combating Cyber Crime 2015 ❖ Amended Media Law of 2008
Malaysia	❖ Sedition Act 1948 ❖ Sedition (Amendment) Act 2015 ❖ Communications and Multimedia Act 1998 ❖ Federal Constitution ❖ Anti-Fake News Act (AFNA) 2018 *(now due to be repealed)*
Myanmar	❖ Penal Code ❖ Telecommunications Law 2013 ❖ Official Secrets Act 1923

Philippines	❖ Revised Penal Code ❖ Cybercrime Prevention Act 2012 ❖ 'Anti-False Content' Bill *(not in force)*
Singapore	❖ Penal Code ❖ Defamation Act 2014 ❖ Administration of Justice (Protection) Act ❖ Protection from Online Falsehoods and Manipulation Act 2019
Thailand	❖ Criminal Code ❖ Computer-related Crimes Act B.E. 2560 (2017) ❖ Civil Procedure Code ❖ Organic Law on the Constitutional Court (2018) ❖ Cybersecurity Act B.E. 2562 (2019)
Vietnam	❖ Penal Code of 1999 ❖ Penal Code of 2015 ❖ Law on Cybersecurity 2018 ❖ Decree No. 72 on the management, provision and use of Internet services and online information (2013) ❖ Draft Decree Implementing the Law on Cybersecurity (2018)

Cases referenced in this report involved the following individuals:

- Alexander Adonis
- Angkhana Neelapaijit
- Anindya Joediono
- Anuphong Phanthachayangkun
- Asheeq Ali Sethi Alivi
- Alex Au
- Ali Abd Jalil
- Arun Kasi
- Azham Akhtar Abdullah
- Ban Samphy
- Brad Bowyer
- Clare Rewcastle Brown
- Daniel De Costa
- Dao Quang Thuc
- Eric Liew
- Eric Paulsen
- Eugene Thuraisingam
- Fadiah Nadwa Fikri
- Fahmi Reza
- Houayheuang Xayabouly
- Isma-ae Tae
- John Tan
- Jolovan Wham
- Karn Pongpraphapan
- Kay Khine Tun

- Khalid Mohd Ismath
- Kheang Navy
- Ko Swe Win
- Kovit Wongsurawat
- Kyaw Soe Oo
- Le Van Sinh
- Leni Robredo
- Li Shengwu
- Lod Thammavong
- Maria Ressa
- Maung Saung Kha
- Min Htin Ko Ko Gyi
- Muhammad Amirul Azwan Mohd Shakri
- Nan Win
- Ngamsuk Rattanasatiean
- Nguyen Nang Tinh
- Nguyen Ngoc Anh
- Nguyen Quoc Duc Vuong
- Nguyen Van Cong Em
- Nguyen Van Phuoc
- Nur Alia Astaman
- Nyein Chan Soe
- Pai Dao Din
- Paing Phyo Min
- Paing Ye Thu
- Pham Xuan Hao
- Phongsak

- Roy Ngerng
- Reynaldo Santos Jr.
- S. Arutchelvan
- Sarinee Achavanuntakul
- Sasiwimol
- Shahiransheriffuddin
- Somphone Phimmasone
- Soukane Chaithad
- Su Yadanar Myint
- Suchanee Rungmuanporn
- Sutharee Wannasiri
- Suthasinee Kaewleklai
- Terry Xu
- Thanakorn
- Thiansutham
- Uon Chhin
- Vichai
- Wa Lone
- Wan Ji Wan Hussin
- Watana Muangsook
- Yeang Sothearin
- Zaw Lin Htut
- Zayar Lwin
- Zunar

Commission Members
March 2019 (for an updated list, please visit www.icj.org/commission)

President:
Prof. Robert Goldman, United States

Vice-Presidents:
Prof. Carlos Ayala, Venezuela
Justice Radmila Dragicevic-Dicic, Serbia

Executive Committee:
Justice Sir Nicolas Bratza, UK
Dame Silvia Cartwright, New Zealand
(Chair) Ms Roberta Clarke, Barbados-Canada
Mr. Shawan Jabarin, Palestine
Ms Hina Jilani, Pakistan
Justice Sanji Monageng, Botswana
Mr Belisário dos Santos Júnior, Brazil

Other Commission Members:
Professor Kyong-Wahn Ahn, Republic of Korea
Justice Chinara Aidarbekova, Kyrgyzstan
Justice Adolfo Azcuna, Philippines
Ms Hadeel Abdel Aziz, Jordan
Mr Reed Brody, United States
Justice Azhar Cachalia, South Africa
Prof. Miguel Carbonell, Mexico
Justice Moses Chinhengo, Zimbabwe
Prof. Sarah Cleveland, United States
Justice Martine Comte, France
Mr Marzen Darwish, Syria
Mr Gamal Eid, Egypt
Mr Roberto Garretón, Chile
Ms Nahla Haidar El Addal, Lebanon
Prof. Michelo Hansungule, Zambia
Ms Gulnora Ishankanova, Uzbekistan
Ms Imrana Jalal, Fiji
Justice Kalthoum Kennou, Tunisia
Ms Jamesina Essie L. King, Sierra Leone
Prof. César Landa, Peru
Justice Ketil Lund, Norway
Justice Qinisile Mabuza, Swaziland
Justice José Antonio Martín Pallín, Spain
Prof. Juan Méndez, Argentina
Justice Charles Mkandawire, Malawi
Justice Yvonne Mokgoro, South Africa
Justice Tamara Morschakova, Russia
Justice Willly Mutunga, Kenya
Justice Egbert Myjer, Netherlands
Justice John Lawrence O'Meally, Australia
Ms Mikiko Otani, Japan
Justice Fatsah Ouguergouz, Algeria
Dr Jarna Petman, Finland
Prof. Mónica Pinto, Argentina
Prof. Victor Rodriguez Rescia, Costa Rica
Mr Alejandro Salinas Rivera, Chile
Mr Michael Sfard, Israel
Prof. Marco Sassoli, Italy-Switzerland
Justice Ajit Prakash Shah, India
Justice Kalyan Shrestha, Nepal
Ms Ambiga Sreenevasan, Malaysia
Justice Marwan Tashani, Libya
Mr Wilder Tayler, Uruguay
Justice Philippe Texier, France
Justice Lillian Tibatemwa-Ekirikubinza, Uganda
Justice Stefan Trechsel, Switzerland
Prof. Rodrigo Uprimny Yepes, Colombia

ISBN 978-92-9037-263-9

International Commission of Jurists

P.O. Box 91
Rue des Bains 33
Geneva
Switzerland

t: +41 22 979 38 00
f: +41 22 979 38 01
www.icj.org