

EXECUTIVE SUMMARY

Dawn of Digital Dictatorship: Weaponizing the Law Against Online Speech in Southeast Asia



What is the ASEAN Regional Coalition to #StopDigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship was established in 2020, by human rights and digital rights activists from Southeast Asia, on a mission to decolonize digital rights and restore our online democracies.

Together, we stand in solidarity with one another, with people from the Global Majority, resisting and pushing back against authoritarian governments and complicit tech companies.

We tell our realities from the ground, and we develop solutions together.

Our truths. Our Stories. Our Solutions. Our Liberation.

Fighting back online authoritarianism in Southeast Asia is, and shall always be, decolonial, grounded on feminist values, centred on our voices and our collective power.

Listed alphabetically, members of the Coalition include: ALTSEAN-Burma, Cambodian Center for Human Rights, ELSAM, Free Expression Myanmar, Foundation for Media Alternatives, ILGA Asia, Manushya Foundation, The Rohingya Maiyafuñor Collaborative Network, SAFEnet, Viet Tan, and Women's Peace Network.

Contact:

ASEAN Regional Coalition to #StopDigitalDictatorship

Coordination: Manushya Foundation

Email: WeAreManushyan@manushyafoundation.org

Citation:

ASEAN Regional Coalition to #StopDigitalDictatorship, Dawn of Digital Dictatorship: Weaponizing the Law against online speech in Southeast Asia, (March 2024)

Copyright

@ManushyaFoundation2024

This work is licensed under Creative Commons Attribution-NonCommercial- NoDerivatives 4.0 International Public License ("Public License"). To view a copy of this license, visit:<https://creativecommons.org/licenses/by-nc-d/4.0/legalcode>

Table of Contents

5	List of Abbreviations
7	Acknowledgements
9	Chapter I. What is the ASEAN Regional Coalition to #StopDigitalDictatorship?
12	Chapter II. Methodology
14	Chapter III. Summary of International Human Rights Laws and Standards
18	Chapter IV. Executive Summary: A Regional Overview
38	Chapter V. Recommendations
39	Recommendations to Governments
41	Recommendations to Members of Parliament
42	Recommendations to Tech Companies
45	Recommendations to Civil Society
46	Glossary

List of Abbreviations

AJPA	Administration of Justice (Protection) Act
AFP	Armed Forces of the Philippines
ASEAN	Association of Southeast Asian Nations
CCA	Computer Crime Act
CIJ	Centre for Independent Journalism
CMA	Communications and Multimedia Act
CNRP	Cambodia National Rescue Party
CPP	Cambodian People's Party
CPV	Communist Party of Vietnam
DCHCP	Department of Cybersecurity and High-tech Crime Prevention
DICT	Department of Information and Communications Technology
ESO	Electronic system operator
ETL	Electronic Transactions Law
FIDH	International Federation for Human Rights
HRD	Human rights defender
ICCPR	International Covenant of Civil and Political Rights
IFJ	International Federation of Journalists
ICJ	International Commission of Jurists
IP	Indigenous people
ISOC	Internal Security and Operations Command
ISP	Internet service provider
KPK	Corruption Eradication Commission
LPRP	Lao People's Revolutionary Party
LPSK	Witness and Victim Protection Agency
KOMINFO	Ministry of Communication and Information Technology
MCIT	Ministry of Communication and Information Technology
MCMC	Malaysian Communications and Multimedia Commission
MIC	Ministry of Information and Communication

MPTC	Ministry of Posts and Telecommunications
MPS	Ministry of Public Security
MNHRC	Myanmar National Human Rights Commission
MoI	Ministry of Information
NEC	National Election Committee
NGO	Non-governmental organisation
NIG	National Internet Gateway
NLD	National League for Democracy
NTC	National Telecommunications Commission
NUG	National Unity Government
NUJP	National Union of Journalists of the Philippines
OHCHR	Office of the United Nations High Commissioner for Human Rights
PAP	People's Action Party
PAS	Malaysian Islamic Party
POFMA	Protection from Online Falsehoods and Manipulation Act
PPPA	Printing Presses and Publications Act
PN	Perikatan Nasional
RGC	Royal Government of Cambodia
RPC	Revised Penal Code
SAC	State Administration Council
SLAPP	Strategic lawsuit against public participation
SUHAKAM	Human Rights Commission of Malaysia
TLHR	Thai Lawyers for Human Rights
TOC	The Online Citizen
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNWGAD	United Nations Working Group on Arbitrary Detention
VNNIC	Vietnam National Internet Center

Acknowledgements

Manushya Foundation and the ASEAN Regional Coalition to #StopDigitalDictatorship would like to sincerely thank everyone who offered their untiring support and unique insight into the digital rights situation in Southeast Asia, and helped to make this report complete and possible.

Manushya Foundation, in particular, would like to express its deep appreciation to all ASEAN Regional Coalition members for their invaluable support and inputs throughout the phases of the research, from identifying the human rights issues to documenting, collecting, and analysing data for various cases, and developing this report, over the past four years. Our heartfelt gratitude extends to both the founding members and new members, who have played critical roles in resisting digital dictatorship and advancing democratic values. Listed alphabetically, they include: **ALTSEAN-Burma, Cambodian Center for Human Rights, ELSAM, Free Expression Myanmar, Foundation for Media Alternatives, ILGA Asia, Jean Linis-Dinco, Manushya Foundation, The Rohingya Maìyafuìnor Collaborative Network, SAFEnet, Viet Tan, and Women’s Peace Network.**

Manushya Foundation and the members of the ASEAN Regional Coalition to #StopDigitalDictatorship express particular gratitude to Manushya’s Digital Rights Team for their coordination, review, editing, and finalisation of the report. Overseen by Emilie Palamy Pradichit (Founder & Executive Director, Manushya Foundation), and Ni Putu Candra Dewi (Advocacy and Campaign Associate on Democracy and Digital Rights, Manushya Foundation), the team includes: Tricia Ho Sze Mei, Ploypitcha Uerfuer, Luna Marciano, Fitri Lestari, Delasari Krisda Putri, Deena Bhanarai, and Arianne Joy Fabregas.

The visual aids within this report, including data visualisations, trend summaries, case study profiles,

and theme overviews, were developed by Luna Marciano and Deena Bhanarai. Additionally, the graphics and illustrations you see would not have been possible without the patience and artistry of our designers. We extend our gratitude to Putu Deoris and Yansanjaya, who were responsible for the layout, case study design, and the creation of all the data visualisation graphics, as well as to Ivana Kurniawati, who illustrated our report and chapter cover pages.

Special gratitude is extended to the former team researchers, volunteers, and interns of Manushya Foundation, who played significant roles through their engagement in conducting desk research and monitoring cases of human rights violations over the past four years. This appreciation is particularly directed to Letitia Visan, Preeyanun Thamrongthanakij, Felicity Salina, Amalia Tihon, and Margaux Bonnard.

We also extend our deep appreciation to Ma Thida from PEN Myanmar, who made significant contributions to the work of the coalition before the illegitimate military coup in Myanmar.

We extend thanks and appreciation to the numerous activists and human rights defenders across the region who have mobilised to defend fundamental human rights with immense courage, often risking their lives in the face of authoritarianism. The debt we owe them has never been greater. Their altruism and courage have been an inspiration for us and a reason more to document the gross human rights violations in the digital space.

This project would not have been possible without the help of the authors below, as well as reviewers who asked to remain anonymous, in validating our desk-research and in some cases, contributing content that informed this report.

No	COUNTRY CHAPTER	ORGANIZATIONS OR NETWORK INDIVIDUALS	INDIVIDUALS
1	CAMBODIA	Cambodian Center for Human Rights (co-author and reviewer); Manushya Foundation (co-author)	xx
2	INDONESIA	Southeast Asia Freedom of Expression Network (SAFE-net) (co-author and reviewer); Manushya Foundation (co-author)	xx
3	LAO PDR	Manushya Foundation	xx
4	MALAYSIA	Manushya Foundation	xx
5	MYANMAR	ALTSEAN-Burma; Free Expression Myanmar; Women's Peace Network (reviewers); Manushya Foundation (co-author)	Anonymous author
6	PHILIPPINES	Foundation for Media Alternatives (author and reviewer); Manushya Foundation (co-author)	xx
7	SINGAPORE	Manushya Foundation	xx
8	VIETNAM	Project 88 (author); Anonymous reviewer	xx
9	THAILAND	Manushya Foundation	xx

Fig. X: Organisations and/or network individuals who were responsible for the writing and reviewing of our country-specific sections under Chapter IV: Country Overviews (Analysis).

Chapter I.

What is the ASEAN Regional Coalition to #StopDigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship, envisioned in 2020 by Emilie Palamy Pradichit, Founder of Manushya Foundation, is an all-star collective consisting of ALTSEAN-Burma, Cambodian Center for Human Rights, ELSAM, Free Expression Myanmar, Foundation for Media Alternatives, ILGA Asia, Manushya Foundation, The Rohingya Maïyafuìnor Collaborative Network, SAFEnet, Viet Tan and Women's Peace Network.

The Coalition’s collective objective is to decolonise the field of Digital Rights, take into account intersectional perspectives with particular focus on marginalised, Global South voices, and fearlessly share our truths. We are stronger together; we share our stories straight from the ground, stand with each other, and work together to envision solutions. All this work is essential in order to preserve what is left of the online and offline freedoms humans still have, and fight back against continued efforts to diminish those freedoms.

#WhatIsHappeningInSoutheastAsia?

The digital space is quickly emerging as one of the key spaces in which human rights are threatened. In Southeast Asia, the internet is no longer a free, safe, and secure space for expression. Restrictive legislation, intimidation, the weaponisation of COVID-19, and even the murder of human rights defenders, activists, and journalists tarnishes the commitment to freedom of expression of the countries in the region. In this light, the need for our rights to be respected, including online, becomes greater.

The collaborative work of the ASEAN Regional Coalition to #StopDigitalDictatorship (“the Coalition”) is to respond to the growing digital repression. After its establishment in 2020, with the coordination of Manushya Foundation, virtual discussions were initiated to discuss challenges faced, while determining collaborative and inclusive efforts to assess, amend, and monitor implementation of legislations affecting digital rights. The Coalition has established itself as a leading regional expert voice on digital rights in the region and is now a key player, powering local and regional voices to speak their truth to power and to resist digital dictatorship.

A core group of members of the Coalition has collectively developed the research and analysis framework of a regional ASEAN Study covering nine Southeast Asian countries: Cambodia, Indonesia, Lao PDR (Laos), Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam. The aim of the ASEAN Coalition’s work goes far beyond merely analysing the legal framework related to freedom of expression online and documenting rights violations in the nine Southeast Asian countries. The main goal is to increase public understanding of how important digital rights are to everyone’s lives and to strengthen netizens’ knowledge of those rights. But there is more to consider. As intersectional feminists, we recognise the internet is not equal for everyone. While the digital realm offers immense opportunities, it is far from being neutral or egalitarian, and it remains susceptible to persistent backlash against the rights of women and LGBTIQ+ people. Like other social spaces, it reflects and reproduces power relations and inequalities, including those related to gender.

Our Intersectional Approach, grounded on Feminist Values & Lived Experiences from the Global South

Coalition members dedicate their work to make Asia a safe and peaceful place for all. While they have different goals and perspectives, the cultivation of an open, safe, and inclusive digital space for all is a

key priority for them. At Manushya Foundation, we place “equality” at the core of our activities, apply a gender lens to all of our work, and focus on powering women activists and human rights defenders, youth,

What is the ASEAN Regional Coalition to #StopDigitalDictatorship?

The ASEAN Regional Coalition to #StopDigitalDictatorship was established in 2020, by human rights and digital rights activists from Southeast Asia, on a mission to decolonise digital rights and restore our online democracies.

Together, we stand in solidarity with one another, with people from the Global Majority, resisting and pushing back against authoritarian governments and complicit tech companies.

We tell our realities from the ground, and we develop solutions together.

Our truths. Our Stories. Our Solutions. Our Liberation.

Fighting back online authoritarianism in Southeast Asia is, and shall always be, decolonial, grounded on feminist values, centred on our voices and our collective power.

and LGBTIQ+ individuals to tell their very own stories in a powerful manner for their advocacy. Likewise, ILGA Asia, a regional federation of more than 204 member organisations, works for the equality of all people regardless of sexual orientation, gender identity, and sex characteristic, as well as liberation from all forms of discrimination and stigmatisation. Women's Peace Network has "equality" as one of its core visions and works to protect the rights and increase the inclusion of marginalised women, youth, and communities in the Rakhine state and across

Myanmar. The Foundation for Media Alternatives focuses on the intersection between information and communication technology (ICT) and gender rights, including tech-related gender-based violence.

We also recognise that gender inequality intersects with other forms of oppression, such as race, class, sexuality, and disability, and women exposed to intersecting forms of discrimination are particularly vulnerable to violence in the digital world. Understanding the intricate ways in which power operates, we apply an intersectional feminist lens to explore and tackle the multifaceted dynamics within the digital realm. Through our work, we shed light on this and the patriarchal power dynamics that hold our world back from fulfilling a society where everyone is treated with fairness and dignity.

However, that is not where our work ends. The ultimate objective is to call, as a strong and unified voice, on governments, policy-makers, and tech companies to move the needle forward from commitments on paper to concrete measures to respect their international human rights obligations—in order to restore our only democracy. Recommendations are also extended to civil society, which provides a critical foundation for holding governments and businesses accountable, and promoting human rights and democracy.

Creating a safe internet space for everyone is crucial for promoting inclusivity, respect, and equal opportunities. Only together can we foster a more inclusive and respectful internet culture where everyone can engage, express themselves, and participate without fear of discrimination or harassment. None of us are free until we are all free.

Chapter II.

Methodology

This Regional Overview is the Executive Summary of the ASEAN Regional Coalition to #StopDigitalDictatorship's first flagship report 'Dawn of Digital Dictatorship: Weaponising the Law Against Online Speech in Southeast Asia'. The report is a culmination of four years of monitoring, research, writing, reviewing, and examining the digital rights space in nine ASEAN countries: Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, The Philippines, Singapore, Thailand, and Vietnam. Our research does not cover Brunei Darussalam and Timor-Leste due to the lack of coalition members in these countries.

The methodology used in the report encompasses both primary and secondary sources. Primary data was gathered by Manushya Foundation, together with organisation members of the ASEAN Regional Coalition to #StopDigitalDictatorship. We have entrusted our coalition members to write thorough country-specific analyses, based on their expertise in the digital rights landscapes of their respective countries. It must thus also be noted that as these coalition members are specialists in their own rights, with a wealth of information obtained through lived experiences and field research, not every source will be cited, as a lot of information was first-handedly provided by the author and not obtained from elsewhere. Please find a list of the organisations and/or network individuals who were responsible for the writing and reviewing of our different Chapter IV country-specific subchapters in **Fig. X (p.8)**.

We included voices from the ground and experts' insight from panel discussions, including sessions we held as part of RightsCon, such as the 2022 "Thailand: Digital Authoritarianism Rising" session, the 2021 "Online Freedom Under Attack: Weaponising Misinformation, Disinformation, and 'Fake News' for Censorship in Southeast Asia" session, as well as a series of other webinars hosted by the Coalition. Participants of the webinars and discussions consisted of citizens, experts, representatives of academia, and civil society groups. For some countries, our Coalition members also conducted independent investigations and compiled data from open sources published by the relevant authorities, government agencies and the judiciary. The report's coverage spans the years 2020 through 2023, except for the chapter on Laos (**Chapter IV, 3. Lao PDR**), where egregious human rights breaches instances prior to 2020 are also included. We focused our inquiries on different target areas, which were ultimately synthesised into

primary themes featured in the reports in this series: criminalisation of defamation and lack of human-centred cyber laws and policies; online monitoring and content moderation; threats to privacy and data protection; harassment of activists and human rights defenders (HRDs); and internet shutdowns.

This report is also composed on the basis of desk research, including a systematic literature review of relevant legislation and regulations; reports, studies, and recommendations by UN human rights mechanisms and NGOs; online news articles; policy and white papers; and independent publications. Data was also obtained from studies and external civil society organisations. We carried out interviews with a wide range of stakeholders to receive the most accurate insight on the state of digital rights on the ground relating to the target areas specified above. The study's ultimate objective is to provide a comprehensive analysis on the state of digital rights in the Southeast Asia region, including during the COVID-19 pandemic, by looking at existing national laws, policies and measures; recorded cases of violation; as well as previous recommendations or proposals made in line with international human rights laws and standards.

Chapter III.

Summary of International Human Rights Laws and Standards

Fig. G: Summary table of international human rights laws and standards.

FREEDOMS OF EXPRESSION AND TO HOLD OPINION		
International Human Rights Instruments	Relevant Provisions and Interpretations	Ratification/Voting/Adoption Date and Status
UDHR	Article 19: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”	NOT Binding but serves as a cornerstone for the development and evolution of international human rights law. as a matter of customary international law
ICCPR	Article 19: Upholds the right of every individual to freedom of expression, including the freedom to “seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media” without interference.	Ratified Cambodia (May 26, 1992) Indonesia (Feb. 23, 2006) Lao PDR (Sept. 25, 2009) Philippines (Oct. 23, 1986) Thailand (Oct. 29, 1996)
	Article 19(3): Articulates a three-part test, stipulating that any restrictions on expression must be “provided by law”, proportionate, and necessary for “respect of the rights and reputations of others,” “for the protection of national security or of public order, or of public health and morals.”	General comment no. 34: Article 19 (freedoms of opinion and expression): States that criminalize defamation must decriminalize it given that “imprisonment is never an appropriate penalty” for, and is neither necessary nor proportionate to the aim of protecting others. ²
UDHR	Article 12: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”	NOT Binding but serves as a cornerstone for the development and evolution of international human rights law. Binding as a matter of customary international law

Fig. G: Summary table of international human rights laws and standards.(continuous)

<p>ICCPR</p>	<p>Article 17: “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.” It also upholds the right of persons to receive legal protection from such interference or attacks.</p> <hr/> <p>General comment no. 16: Article 17 (right to privacy): This Article is intended to protect against said infringements, both by states and private individuals. Further, “interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.” The principles of legality, necessity and proportionality also apply to privacy limitations.³</p>	<p>Ratified Cambodia (May 26, 1992)</p> <p>Indonesia (Feb. 23, 2006)</p> <p>Lao PDR (Sept. 25, 2009)</p> <p>Philippines (Oct. 23, 1986)</p> <p>Thailand (Oct. 29, 1996)</p> <p>Vietnam (Sept. 24, 1982)</p> <p>Not signed or ratified Malaysia, Myanmar, Singapore</p>
<p>Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2016) juncto Report of the OHCHR on the right to privacy in the digital age (2014)</p>	<p>Legitimate surveillance, where intended to limit the freedom of expression, requires states to demonstrate the risk that the expression “poses to a definite interest in national security or public order.”⁴ All interference with the right to privacy must also be authorised by an independent oversight body through careful review, and be accompanied with an assurance of effective remedy in case of a breach.⁵</p>	<p>Non-binding (interpretive)</p>
<p>RIGHTS OF HRDS</p>		
<p>International Human Rights Instruments</p>	<p>Relevant Provisions and Interpretations</p>	<p>Ratification/Voting/Adoption Date and Status</p>
<p>UN Declaration on Human Rights Defenders</p>	<p>Article 6: Provides for the right of persons to seek, obtain, receive and hold information about all human rights and fundamental freedoms; freely publish or impart or disseminate information and knowledge on all human rights and fundamental freedoms; and to study, discuss and hold opinions on the observance of these rights.</p> <p>Article 7: “Everyone has the right, individually and in association with others, to develop and discuss new human rights ideas and principles and to advocate their acceptance.”</p> <p>Article 9: Everyone whose rights or freedoms pursuant to the Declaration are allegedly violated must be able to access an effective remedy and have their complaint heard by an independent, impartial and competent authority.</p>	<p>NOT Binding but serves as a cornerstone for the development and evolution of international human rights law</p>

Fig. G: Summary table of international human rights laws and standards.(continuous)

RIGHT TO AN EFFECTIVE REMEDY		
International Human Rights Instruments	Relevant Provisions and Interpretations	Ratification/Voting/Adoption Date and Status
UDHR	Article 8: “Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.	NOT Binding but serves as a cornerstone for the development and evolution of international human rights law
ICCPR	Article 2(3): Provides for the obligation of states to ensure that those individuals whose rights have been violated have access to an effective remedy whether the violation(s) were committed by a person acting in their official capacity. Further, the effective remedy is to be determined by a competent judicial, administrative, legislative or other authority as mandated by the national legal system. The bottomline is that, regardless of the authority in charge, remedy must actually be granted.	<p>Ratified</p> <p>Cambodia (May 26, 1992)</p> <p>Indonesia (Feb. 23, 2006)</p> <p>Lao PDR (Sept. 25, 2009)</p>
	General comment no. 31 (the nature of the general legal obligation imposed on States Parties to the Covenant): Judicial and administrative mechanisms must be set in place to “investigate allegations of violations promptly, thoroughly and effectively through independent and impartial bodies.” Reparation to individuals can take the forms of “restitution, rehabilitation and measures of satisfaction, such as public apologies, public memorials, guarantees of non-repetition and changes in relevant laws and practices, as well as bringing to justice the perpetrators of human rights violations.” ⁷	<p>Philippines (Oct. 23, 1986)</p> <p>Thailand (Oct. 29, 1996)</p> <p>Vietnam (Sept. 24, 1982)</p> <p>Not signed or ratified Malaysia, Myanmar, Singapore</p>

Chapter IV.

**Executive Summary:
A Regional Overview**

SYMBOL KEY:

Implications and issues faced by victims of Digital Dictatorship

Digital Dictatorship tactics used against victims:

- 🧠 Psychological violence (e.g. harassment, threats against personal safety, attacks on loved ones, torture, summons and/or intimidating questionings) used against victims
- 📧 Smear campaigns, online hate, and/or online bullying used against victims.
- 🔪 Physical violence (e.g. assassinations/attempted assassinations, physical attacks) used against victims
- 👏 Strategic Lawsuit Against Public Participation (SLAPP) cases used against victims
- 🔒 Immigration issues and/or Transnational Repression (TNR) used against victims, and/or victims forcefully displaced/made into refugees
- 💰 Victims fined
- 🚔 Victims charged, arrested, and/or jailed/imprisoned
- 👁️ Victims reported being surveilled

Justifications used when victims are accused of Incitement, Defamation, and/or spreading Disinformation

- 🗣️ Victim accused of committing a crime by criticising authorities, the state, and/or other individuals with power
- 👑 Victim accused of committing lèse-majesté (i.e. insult or defamation against the monarchy)
- 🇻🇳 Victim accused of committing incitement against a one-party authority (e.g. against the one-party Socialist authority of Vietnam)
- 🙏 Victim accused of committing a crime by committing religious treason, and/or being 'socially unacceptable' and/or 'deviant of dominant social norms'

The victims are part of marginalised/exceptionally targeted groups:

- 💙 Rohingya, and/or other marginalised ethnic, racial, and religious groups
- 💜 Women and other gender-marginalised identities
- 🏳️‍🌈 LGBTIQ+ community
- 🇺🇸 HRDs fighting for COVID-19 related transparency (particularly during the lockdown period)
- 🏢 HRDs fighting for Corporate Accountability/Politician Accountability
- 🌱 HRDs for Climate Justice
- 📰 Journalists

Fig. A1: Symbol key for implications and issues faced by victims of Digital Dictatorship

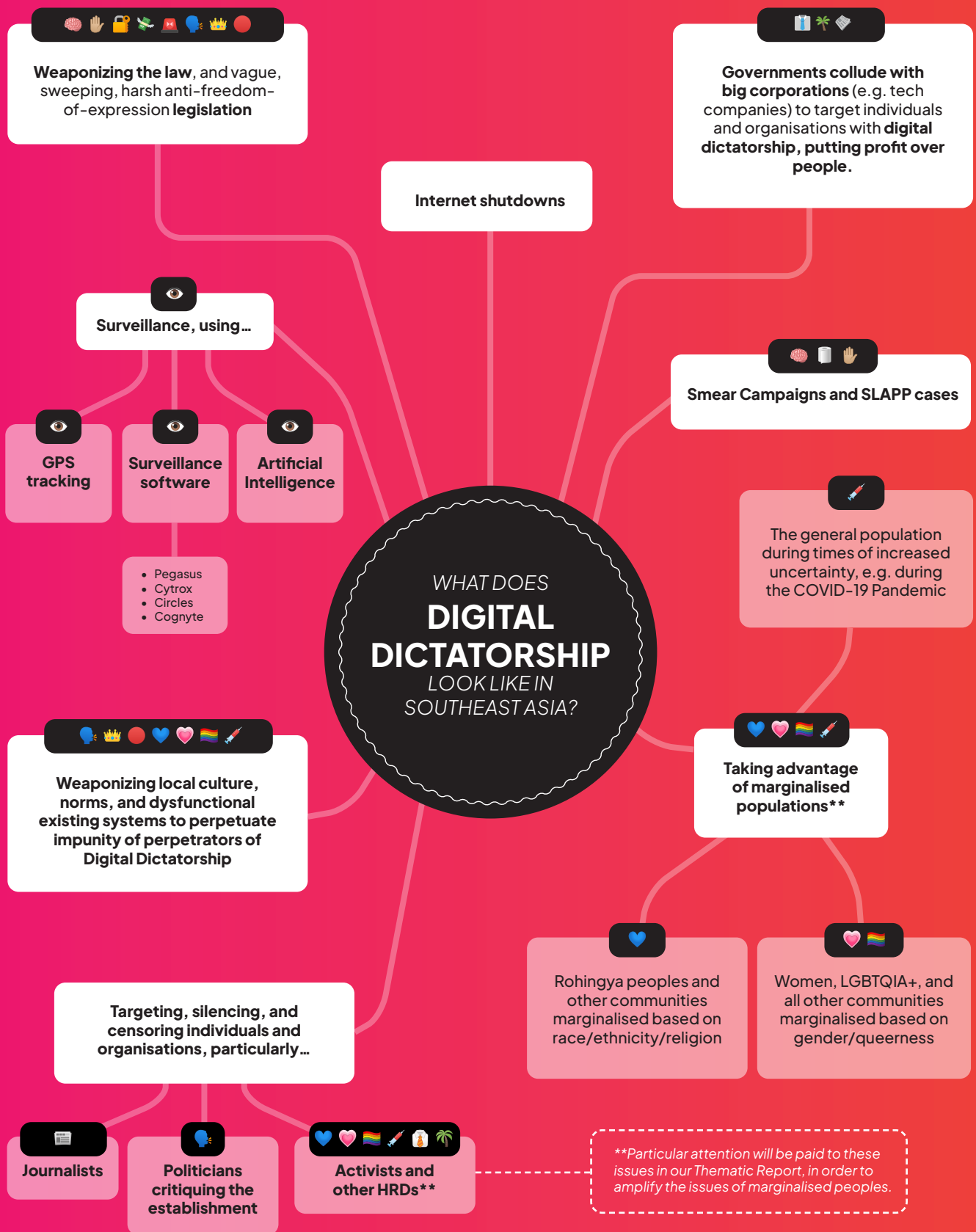


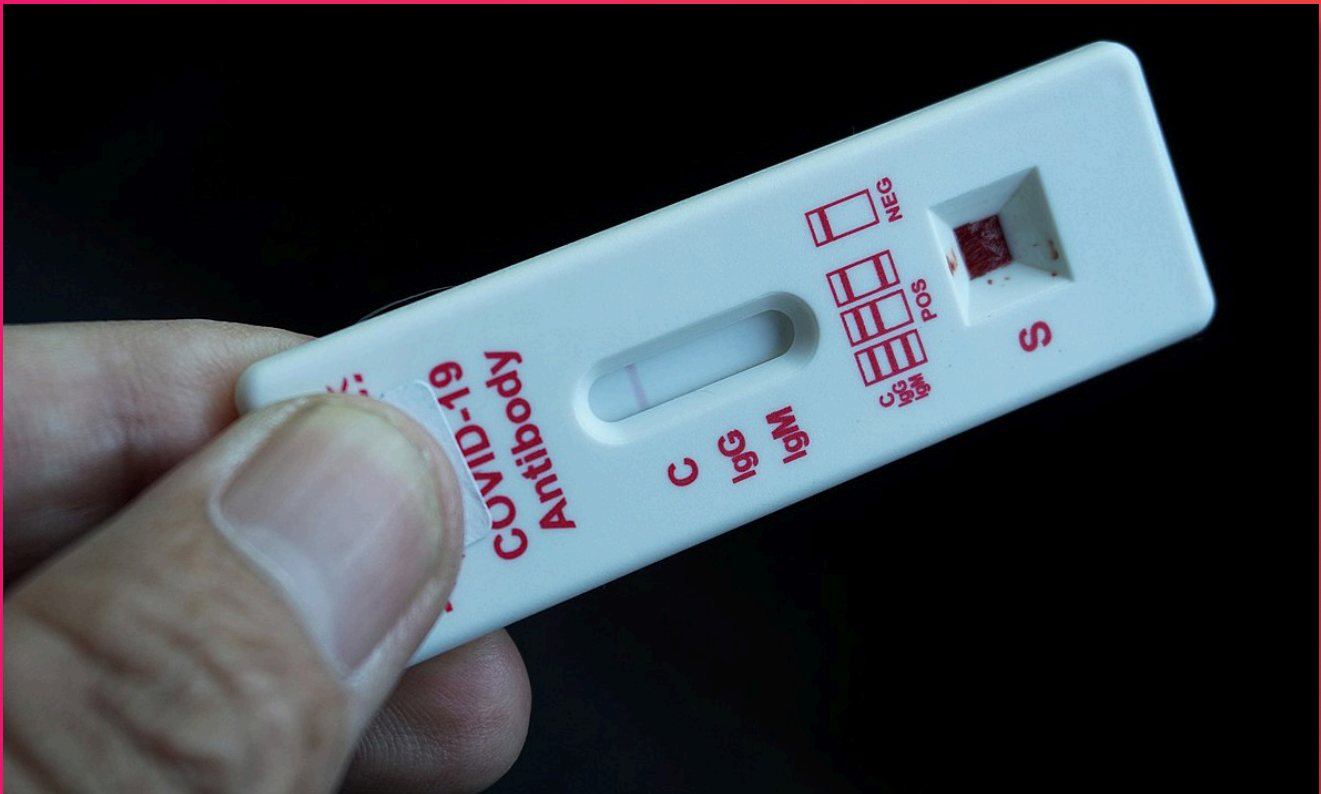
Fig. A2: Symbol key for implications and issues faced by victims of Digital Dictatorship

The Internet is a powerful tool used by many people in the world. It helps us communicate, conduct mundane activities, but it equally facilitates our access to information, the ability to share opinions, engage in debate, and be active participants in our societies. However, the power of the Internet is a double-edged sword. Just as power can be wielded to improve life for humans, it can also be abused to do harm and oppress. There has been a global effort to create global standards and norms, as well as regional and country-based legislation that effectively regulate online space and internet use. Regulating online space and also technology companies is crucial, as self-regulation has proved insufficient to manage the complexities and impacts of their activities on society. The technology industry must be held to account, not only in terms of growth and profits, but also for its impact on society and the environment. This regulation will help guide administrators and users on how to shape the Internet to make it safe, respectful and useful for all.² Unfortunately, some states are taking this as an opportunity to implement new ways to oppressively control their populations, under the guise of ‘national security’ and ‘improving the safety’ of the internet and the jurisdiction. This might come in the form of oppressive governments creating new legislation that unreasonably and inhumanely controls the

people, or in the form of these governments abusing existing ‘loopholes’ in legislation to do so. This is what is referred to as ‘digital authoritarianism’ or ‘digital dictatorship.’

Digital authoritarianism is exceptionally prevalent in Southeast Asian countries, where governments have long failed to safeguard certain human rights of their citizens. Some human rights that are still being severely withheld from many Southeast Asian people include their rights to freedom of speech, to information, and to privacy. The goal of this report is to paint a detailed picture of digital repression and the rise of digital dictatorship in Southeast Asia over four years, from 2020 until the end of 2023.

The use of vague and expansive laws to criminalise legitimate online speech have given governments sweeping monitoring powers over the digital space and communication. Laws such as lèse-majesté, sedition, defamation, hate speech, and criminalisation of fake news are just a few of the offences invoked to threaten and punish individuals for speaking the truth or sharing their opinions. Moreover, governments evidently took advantage of the COVID-19 pandemic and lockdown to implement laws and policies that regress democracy, violate human rights, and further entrench repressive measures.



Rapid test method - © Heru sutimbul (https://commons.wikimedia.org/wiki/File:Hasil_Rapid_Test.jpg)

Digital Dictators take advantage of the masses during times of heightened uncertainty, paranoia, and fear, for example, during the COVID-19 Pandemic

The COVID-19 pandemic undeniably increased anxiety, paranoia, and fear levels for people all across the globe. Southeast Asia is no exception. While Southeast Asian governments responded to the people's emergency needs to an extent, many simultaneously took the pandemic, particularly during the global lockdown period, as an opportunity to impose more restrictions on their peoples' freedoms. The increased practice of 'social distancing' and 'work-and-learn-from-home' practices led to more human reliance on the internet, online platforms, and information technology in general. Because of this reliance, digital dictators were effectively able to exploit IT for mass digital dictatorship. This took the forms of passing and abusing State of Emergency Decrees (such as in Cambodia, Malaysia,

and Thailand), creating specialised COVID-19 'task forces' (such as in Laos, Thailand, and Indonesia), increasing surveillance of people's public as well as private movements using software (such as in Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam), and justifying information takedowns and restrictions on people's freedoms as their way of 'combating the spread of false information about COVID-19' ((such as in Lao PDR, Myanmar, the Philippines).



To read more, please see our '**PANDEMIC POLITICS**' discussion boxes included in each country chapter.

Fig. B1: Digital Dictators take advantage of the masses during times of heightened uncertainty, paranoia, and fear, for example, during the COVID-19 Pandemic.

All countries covered in this report have included defamation as a major offence within their criminal and penal codes. For example, in **Cambodia** and **Thailand**, two nations with powerful monarchies, vague and draconian *lèse-majesté* laws are constantly used to stifle dissent. Digital repression has also been observed in **Indonesia**, **Malaysia**, the **Philippines**, and **Singapore**. These countries have separate cyberspace-regulating legislation that weaponize accusations of ‘defamation’ and ‘blasphemy’ in order to silence people.

These measures are often rooted in the view, observed across many Southeast Asian countries, that freedom of expression is an attack against actors including government authority. A particularly complex situation can be witnessed in nations with histories of communist leadership. **Vietnam**, for example, is known as one of the final strongholds of one-party communist rule in the region, with the country being governed by the Communist Party of Vietnam (CPV) since 1976. Though the Vietnamese government’s communist identity makes it stand out in the region, it frequently behaves similarly to its non-communist neighbouring governments. Often under the guise of promoting ‘unity’ among the masses in order to protect the integrity of communism in Vietnam, the government enforces strict controls over the online environment and maintains a strong stance against those expressing opposing views. Similar tactics are used in Vietnam’s communist neighbour, **Lao PDR** (Laos). Laos is also a one-party socialist republic, and the Lao People’s Revolutionary Party (LPRP) has been the only legal political party since 1975. The Lao government notoriously abuses its vaguely written laws in order to silence views, expressed both online and offline, that the government perceives as threatening to its control. More specifically, both Laos and Vietnam use Article 117 of their Penal Code to silence any opposition by punishing anything associated with propagating materials opposing the State.^{3,4}

Communist or non-communist, Southeast Asian governments gravitate to similar oppressive tactics; the only difference between them tends to be the justifications they use for their oppression.

All the aforementioned control tactics are fundamentally rooted in establishing fear, in order to compel the masses into submission. A clear example of this is exhibited through the behaviour of the Myanmar junta, which has continuously cracked down on dissenting voices since it launched a coup on February 1, 2021. It utilises violent measures to establish fear among its masses, in order to discourage opposition. For instance, the Ministry of Transport and Communications ordered in 2019 restrictions on mobile internet in nine townships in Rakhine and Chin States under Section 77 of the Telecommunications Act. Despite partial lifts, irregular enforcement persists. In April 2021, all mobile data and wireless broadband were cut off. In addition, the military junta is instilling fear in the population by destroying everything in its path, affecting 80,000 homes and forcing 3,800,000 civilians to flee their homes. However, the measures put in place also target workers legitimately engaged in essential jobs. More than 20 media groups, including press agencies, publishing houses and printing works, have been banned since the coup. More than 140 journalists have been detained and, tragically, four have lost their lives in custody.⁵

As we have just discussed, efforts to limit freedom of expression and control the flow of information online can be witnessed through instances of censorship of online content, strong hold over tech companies by passing restrictive legislation to control them, and internet shutdowns. Often framed as accidental or due to technical difficulties, governments and other actors often have an intentional, direct hand in creating these interferences. Governments also collude with equally complicit BigTech companies, which often

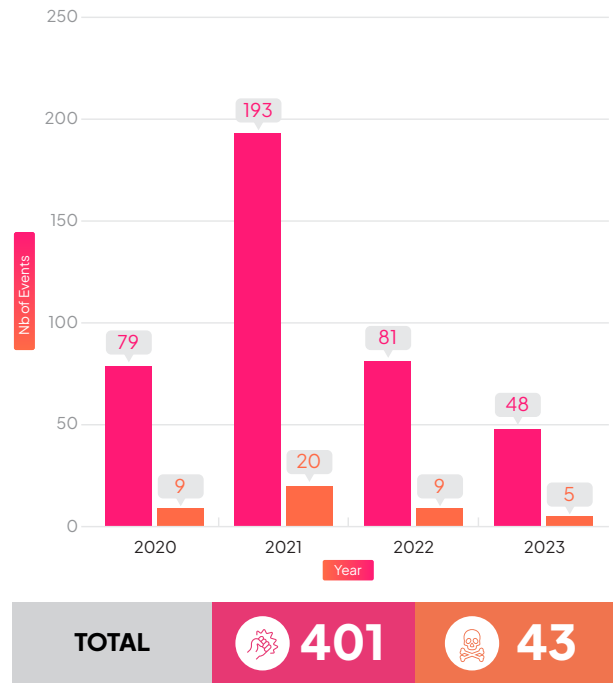
comply with removal requests sent by governments. By complying with these requests, tech companies are complicit in the continuing infringement of freedom of speech and information. For example, Meta received 772 requests for government restrictions in Indonesia in 2020, 1009 in 2021, and 1475 mid-2022. Of these 1475 requests, 1458 restrictions were actually put in place.⁶ As such, they should be held accountable for their roles in obstructing freedom of expression in Southeast Asia.

Aside from creating unsuitable legal frameworks, several countries in the region have been suspected of using spyware to surveil, monitor and punish pro-democracy activists, human rights defenders, journalists, academics, and so on. The cases of **Thailand, Malaysia, Myanmar and Indonesia** highlight how far authoritarian actors are willing to go in order to maintain legitimacy, going as far as using advanced information technology to police its citizens, claiming that this is all necessary in the name of “national security.”

More precisely, Myanmar uses Cognyte software, Thailand relies on Pegasus, Indonesia uses Cyrox and Circles Technology, while Malaysia also relies on Circles technology.

Even in cases where spyware is not used, a common tactic seen among Southeast Asian countries is the overexertion of police power to silence dissent and cover their abuses against journalists. Southeast Asia is known for having very powerful corrupt and powerful law enforcement entities, resulting from Cold War-era militarization of Southeast Asian armed forces by the United States and other geopolitical stakeholders. Southeast Asian police forces use tactics ranging from threats, stalking, doxxing, summoning, and detaining, to physical violence, including assassinations. The targets of these tactics are often people simply trying to express themselves freely online, or trying to practise independent, ethical and transparent

Disorders involving the Media in ASEAN (Indonesia, Myanmar, The Philippines, and Thailand)



The Armed Conflict Location & Event Data Project (ACLED), *Disorder Involving the Media*, (10 February 2024), available at: <https://acleddata.com/data-export-tool/>

LEGEND

- Disorders involving the Media
- Disorders involving Fatalities

Fig. C: Disorders involving the Media in ASEAN (Indonesia, Myanmar, The Philippines, and Thailand), 2020-2023.

i The information used to construct this infographic is sourced from the ACLED database, specifically the dataset titled "Disorders involving Media." Within this database, we have exclusively selected relevant countries from the ASEAN region, namely Indonesia, Thailand, Myanmar, and the Philippines. The events were further filtered based on an additional criterion: date. As our report focuses on events from 2020 to 2023, only those occurring between January 1, 2020, and December 31, 2023, have been included

online journalism, all things that are supposedly recognized by the Universal Declaration of Human Rights. Ironically, it is the police and other armed forces that are the ones committing crimes against international human rights standards, by targeting such individuals. Since the coup, Myanmar has become the world’s second biggest jailer of journalists, behind China.⁷ **Vietnam** has forced many journalists into hiding, or to flee the country.

State officials also frequently sue independent media outlets, and sometimes even abuse their powers to revoke independent media licences altogether. Over the past few years, there have been some particularly high-profile cases coming from **Singapore** and **Cambodia**, where news outlets have had their licences revoked based on counterfeit claims.

In some of the cases, those involved with media outlets were targeted as individuals, such as the case of Terry Xu in **Singapore**—editor of the now-inoperative The Online Citizen (TOC)—who was targeted outside of his involvement with TOC. Many pro-democracy activists, netizens, and prominent figures who have expressed their dissatisfaction with the authoritarian regimes are often targeted by orchestrated efforts to discredit and tarnish their reputation. While not all Southeast Asian countries employ this method, state-led disinformation and smear campaigns have been observed in **Thailand**, **Cambodia**, and **Malaysia**.



Panusaya 'Rung' Sithijirawattanakul - © Adirach Toumlamoon (https://commons.wikimedia.org/wiki/File:Panusaya_Sithijirawattanakul.jpg)

Digital Dictatorship threatens the safety of women, LGBTIQ+, and all other communities marginalised based on gender/queerness

Similar to the aforementioned cases regarding people who have been marginalised based on race, ethnicity, and religion, women and LGBTIQ+ people are targeted based on their identities, even when states claim that they recognize gender equality and LGBTIQ+ rights. Online sexual harassment, smear campaigns, doxxing, forced outings, misogyny, and other gender-based violence, are used in every Southeast Asian nation as weapons against people of marginalized gender and sexuality identities, especially those with intersecting marginalized identities. For example, Malaysian Muslim women's advocates have reportedly been harassed for supporting Muslim women's rights causes, and have been accused of being morally 'deviant' for doing so.¹ It must also be acknowledged that separate from online harassment, people of marginalised gender/sexuality identities also deal

with disproportionate levels of gender-based and sexuality-based violence if/when incarcerated as a result of Digital Dictatorship. Part of the issue is also likely the lack of representation of diverse gender identities in governments and other decision-making bodies. If societies are disproportionately straight-identifying and patriarchal, they are more likely to cause and/or allow violence against people of marginalised gender and sexuality identities. Overall, women and LGBTIQ+ individuals are disproportionately affected by gender-based harassment and digital dictatorship overall.





i

To read more, please see our '**INTERSECTIONAL GENDER ANALYSIS**' sections at the end of each country chapter.

1. UN Women Asia Pacific, Online Violence Against Women in Asia: A Multicountry Study, (November 2020), available at: <https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAAsia/Docs/Publications/2020/12/ap-ICT-VAWG-report-7Dec20.pdf>

Fig. B2, Intersectional Gender Focus: Digital Dictatorship threatens the safety of women, LGBTIQ+, and all other communities marginalised based on gender/queerness.

In addition to the digital rights infringements faced by netizens at large, marginalised communities within all the nations in question are particularly susceptible to these perils. The online sphere mirrors and perpetuates the power dynamics and inequalities that already existed in the offline space; it is thus no surprise that the challenges experienced by women and LGBTIQ+ individuals and racially/ethnically marginalised communities like the Rohingya peoples are also encountered online. In **Indonesia**, for instance, human rights defenders (HRDs) and activists who express their views online, are subjected to doxxing, intimidation, and slander, to name a few. Likewise, women HRDs and LGBTIQ+ people in **Thailand** experience online attacks and harassment online, in relation to their activism and work. The situation in **Myanmar** is also concerning, with the rampant use of doxxing and smear campaigns used against marginalised communities, often done for elites' political and personal gain. It is widely known that the Rohingya peoples have been targeted in particular by online hate campaigns; in 2022, Amnesty International reported findings that Meta "knew or should have known that Facebook's algorithmic systems were supercharging the spread of harmful anti-Rohingya content in Myanmar," and yet, "still failed to act."⁸ Meta's lack of regulation has allowed for disinformation, misinformation, and overall harmful anti-Rohingya rhetoric to be spread amongst the general population. This cannot be taken lightly; spreading this sort of rhetoric directly fuels the dehumanisation and thus exploitation of the Rohingya peoples, and allows for their continued genocide. Amnesty's findings demonstrate how Meta contributed to all of this.⁹

** Look out for these     symbols in the visual aids included throughout our Thematic Report, which will indicate cases specifically related to/that disproportionately affect the Rohingya, women's and LGBTQIA+ communities, cases related to the COVID-19 pandemic, and others.



Rohingya refugees getting off the boat taking them from Myanmar to Bangladesh, close to Shamlapur village in Cox's Bazar, Bangladesh. 6 September 2017. ©Amnesty International

Digital Dictatorship threatens the safety of the Rohingya peoples, and other groups marginalised based on race, ethnicity, and religion

It is widely known that discrimination based on ethnic, religious, racial, or other grounds - is an oppressive tool of authoritarian nation-state governments. These governments know that in order to increase and maintain the power of the 'elite in-group,' and more easily control the masses, they need to demonise and discriminate against 'out-groups.' In Southeast Asia, many different ethnic, religious, racial, and other groups are socially ostracised. Indigenous communities are often targets of this ostracism, because they are often either Indigenously living on lands that governments and corporations want to exploit, or are viewed by governments as a source of exploitable labour. Notable groups in Southeast Asia include the Indigenous hill tribe peoples of the northern and northeastern Mekong Region, the Indigenous peoples of West Papua, as well as the Indigenous Rohingya peoples. In order to further their discriminatory agendas, authoritarian

governments have exploited social media and surveillance technologies to violate the human rights of these groups. Examples of how this might present itself include orchestrating social media smear campaigns against these marginalised peoples and their allies to intimidate them out of defending these groups, as well as censoring marginalised voices online. For example, the Rohingya peoples have long been targets of online hate campaigns on their own lands, and now increasingly on lands on which they are seeking refuge, such as Indonesia.



To read more, please see our detailed reporting about marginalised groups in our country-specific chapters (e.g. we address Rohingya-related cases as part of our '1. Myanmar' chapter).

Fig. B3, Rohingya Focus: Digital Dictatorship threatens the safety of the Rohingya peoples, and all other communities marginalised based on race, ethnicity, and religion.

Thousands of displaced Rohingya are currently seeking refuge on the coasts of Indonesia, Thailand and Malaysia, fleeing Myanmar. Indonesia, like Thailand and Malaysia, has not signed the 1951 United Nations Convention on Refugees, which sets out legal protections, and is therefore under no legal obligation to accept them. What's more, these Rohingya face hostility from the local population.¹⁰ It is risky enough to be a vocal HRD of any kind in Southeast Asia; HRDs with intersectional marginalised identities are at an even greater risk, as the oppressive bodies will intentionally use hateful, discriminatory language and other forms of violence against them.

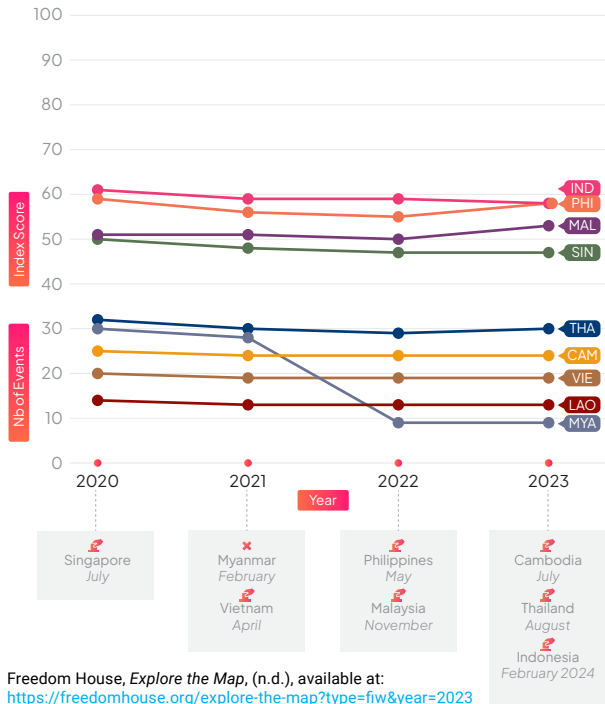
It is paradoxical for Southeast Asian governments to claim that they are champions of human rights and freedom, while allowing these intense abuses to happen against people expressing themselves freely online and offline. There is no need for such pretence while our democracies are clearly under attack in Southeast Asia. According to Freedom House's methodology, and as indicated in each of our Thematic Report chapters, all except four of the Southeast Asian nations mentioned in our Report were considered 'authoritarian' ('not free') states in 2023. The only four that were considered 'semi-authoritarian' ('partly free') were Singapore, Indonesia, Malaysia, and the Philippines; these three were considered 'semi-authoritarian'.¹¹ Thus, it will undeniably take time to fully revolutionise outdated and harmful systemic structures; fixing these complex systems will not happen overnight. However, the complexity of these structures is no excuse for denying people of human rights. If Southeast Asian governments truly wanted to demonstrate their commitment to human rights, they would, at very least, implement effective remedy measures to handle cases of human rights abuses, including implementing procedural safeguards and independent oversight. Right now, no Southeast Asian government has these systems in place at an adequate level. For example,

Cambodia, Malaysia, Myanmar, Singapore, and Vietnam have no specific legislation to protect people from Strategic Lawsuits Against Public Participation (SLAPP), at all. Lao PDR does not even recognise human rights defenders, and does not have any anti-SLAPP measures in place. Indonesia, Philippines, and Thailand are among the few countries who have some anti-SLAPP provisions; however, they are either insufficient, very limited (for example, in the case of the Philippines where provisions are only available regarding environmental cases), or difficult to put into practice because of the inefficient judicial systems in place.

All the above are very concerning symptoms of digital dictatorship. Evidently, oppressive governments across Southeast Asia recognise the power of the internet, surveillance technology, and Artificial Intelligence, and have abused them for their own gain. If digital freedoms are under threat, then human rights are under threat. This is poignantly demonstrated in the way that Freedom House's 'Freedom on the Net' (FOTN) and 'Freedom in the World' (FITW) reports have both depicted declining trends in societal freedoms. The state of democracy (FITW reports) has significantly declined across the world over the past 17 years, while the state of internet freedom (FOTN reports) significantly declined across the world over the past 13 years.¹² Southeast Asia is no exception to these trends. As the following chapters will show, all the Southeast Asian nations covered in our Thematic Report study fall into the 'not free' or 'partially free' categories for both the state of democracy (FITW) and the state of internet freedom (FOTN) indexes, have remained in these categories for the entirety of the 2020 to 2023 period, and have also all experienced collective score declines during this period.¹³ We must not allow ourselves to succumb to these advances of power, and must diligently observe political actions that affect this topic, in order to more effectively collectively demand from

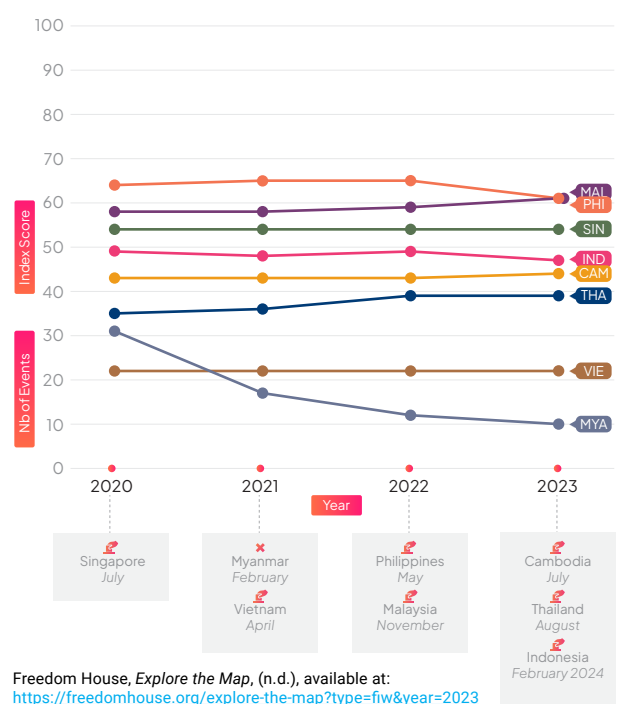
Southeast Asian governing bodies more procedural safeguards, independent oversight, accountability, and overall respect of universal human rights. Oppressive governments are counting on the people to be too afraid or ignorant to advocate for our human rights, so that they can increasingly usurp more power at the expense of our collective freedoms. We must all take digital dictatorship seriously, for it is a lethal tool that forms part of greater dictatorial projects as a whole.

Democratic Status of the Country



Freedom House, *Explore the Map*, (n.d.), available at: <https://freedomhouse.org/explore-the-map?type=fiw&year=2023>

Digital Space & Online Freedom Status



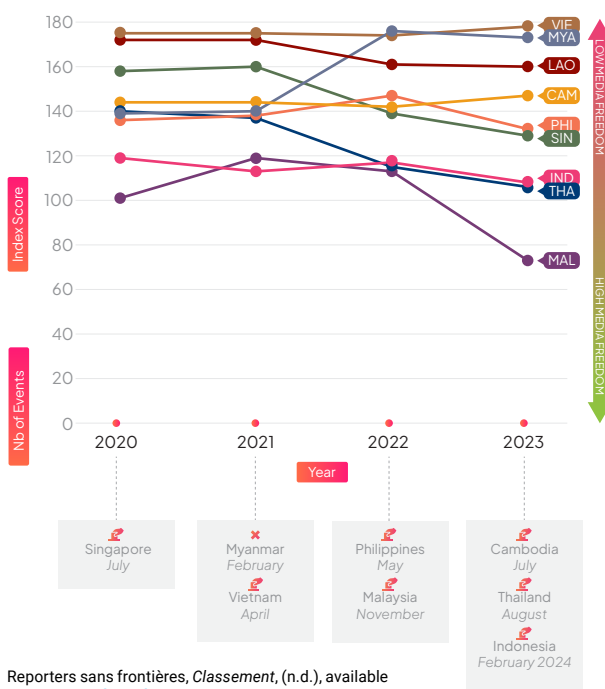
Freedom House, *Explore the Map*, (n.d.), available at: <https://freedomhouse.org/explore-the-map?type=fiw&year=2023>

LEGEND

70–100: Free (F) 40–69: Partial Free (PF) 0–39: Not Free (NF)

Elections Illegitimate coup

Media and Press Freedom Status



Reporters sans frontières, *Classement*, (n.d.), available at: <https://rsf.org/fr/classement>

LEGEND

High media freedom status Low media freedom status

Elections Illegitimate coup

i





Please note that Freedom House and Reporters sans frontières adopt a distinctive method for their yearly assessments. Each assessment corresponds to events from the preceding year. For instance, the decline shown for Myanmar in the 2022 assessment is due to the Illegitimate coup in February 2021.

Fig. D: Data visualisation of Democratic Status, Digital Space and Online Freedom, and Press and Media & Press Freedom Ratings for ASEAN countries acknowledged in this report.

This report will conclude with a series of recommendations for governments, members of the parliament, civil society organisations (CSOs), and tech companies. All of these actors play a key role in safeguarding digital freedoms in Southeast Asia. Governments are responsible for ensuring respect for human rights as stipulated in national and international human rights laws. Members of parliament are the actors who must ensure effective creation and implementation of laws that protect human rights. Tech companies have a distinct responsibility not only to respect human rights, but also to manage risks of human rights harms, aiming to prevent them, and to provide remedies when breaches occur. Finally, CSOs and general members of civil society should continue their informative activities, advocacy, and cross-sector collaboration, as well as support independent evaluations and set up an independent multi-stakeholder body which monitors digital rights abuses.






As suggested earlier, the invention and widespread use of information technology has given humans an immense amount of power. While this power can be used in ways that benefit society as a whole, it is the unfortunate case that many people and institutions are actively choosing to use this power to oppress others, and do harm, for their personal gain. This report aims to paint a detailed picture of what the issues are with the Southeast Asian digital rights landscape, who is responsible for this, why they might be compelled to do it, and how the issues can be remedied. Only after truly understanding how interconnected mechanisms work, can we combat digital dictatorship and push for tangible progress. Human behaviour online is a reflection of human behaviour offline; thus, digital rights are human rights.

Fig. E: List of laws weaponised by ASEAN governments to curb online freedoms through Digital Dictatorship, and justifications for their usage.

	 CAMBODIA	 INDONESIA	 LAOS	 MALAYSIA
Sedition	Article 494 - Criminal Code	Sedition was declared as "unconstitutional" (2007)	Article 297 - Penal Law	Section 3 - Sedition Act (2015) Communications and Multimedia Act (1998)
Defamation	Articles 305 to 308 - Criminal Code Article 10 - 1995 Press Law	Article 433 & 434 - Criminal Code Article 27(A) - Electronic Information and Transactions (No. 1 of 2024 as the second revision of No. 11 of 2008)	Articles 117, 205 & 206 - Penal Law	Sections 499 to 502 - Penal Code
Lèse-majesté	Article 437bis - Criminal Code	/	/	/
Fake news	Cybercrime Law (2021) Articles 425, 494 & 495 - Criminal Code	Articles 263 & 264 - Criminal Code Article 28 - Electronic Information and Transactions (No. 1 of 2024 as the second revision of No. 11 of 2008)	Article 117 - Penal Code Law on Prevention and Combating Cyber Crime (2015) Decree No. 327 - Internet-Based Information Control/Management (2014)	Anti-Fake News Act (2018) Section 505(b) - Penal Code Section 233 - Communications and Multimedia Act (1998)
ISPS, media, and tech companies	Press Law (1995) Telecommunications Law (2015)	Broadcasting Law (No. 32 of 2002) Electronic Information and Transactions (No. 11 of 2008) Press Law (No. 40 of 1999) Telecommunications Law (No. 36 of 1999)	Telecom Law (2021) Law on Information and Communication Technology No. 02/NA (2016)	Communications and Multimedia Act (1998) Printing Presses and Publication Act (1984) Evidence Act (1950)
Mass surveillance	National Internet Gateway SubDecree (2021)	State Intelligence Law (2011)	SIM Card Registration (2020)	Security Offences (Special Measures) Act (2012) Amended Prevention of Crime Act (2014)
Covid-19 temporary and emergency laws, regulations, task forces.	Section 5 - Law on the Management of the Nation in a State of Emergency (2020) COVID-19 Law (2021) National Committee for Combating COVID-19 (Task Force, January 2020) StopCOVID-19 (Tracking Device, April 2020)	Section 5 - State of Emergency Law (1959) Section 11 - COVID-19 Law (2020) Ministerial Regulation Number 5/2020 on Private Electronic System Operators (MR 5/2020) Satgas Penanganan COVID-19 (COVID Task Force, March 2020) PeduliLindungi (Tracking Device, April 2020)	National Taskforce Committee for COVID-19 Prevention and Control (Task Force, May 2021) Special Task Force (Fake News Task Force, May 2021) LaoKYC (Tracking Device, June 2020)	Emergency (Essential Powers) (No.2) Ordinance (2021) Special Ministerial Committee on COVID-19 (Task Force, March 2020) MySejahtera & MyTrace (Tracking Devices, April 2020)

















The laws and regulations featured on this table don't belong to a single defined category but can also be placed within other categories. While the list is not exhaustive, it captures the essence of the primary legal frameworks in place.













	 MYANMAR	 PHILIPPINES	 THAILAND	 SINGAPORE	 VIETNAM
Sedition	Articles 124A and 505 - Penal Code	Section 9 - Anti-Terrorism Act (2020)	Article 116 - Penal Code	Sedition Act (1948)	Articles 109 & 117 - Penal Code
Defamation	Articles 499 to 502 - Penal Code Section 66(d) - Telecommunications Law (2013) Section 46 - Anti-Corruption Law (2013) Section 9(g) - News Media Law (2014)	Articles 353 to 358 - Penal Code Section 4(c)(4) - Cybercrime Prevention Act (2012)	Articles 326 to 333 - Penal Code	Sedition Act (1948) Sections 499 to 500 - Penal Code	Articles 155 to 156 - Penal Code
Lèse-majesté	Lèse-majesté is no longer in effect (2019)	/	Article 112 - Penal Code	/	/
Fake news	Article 68(a) - Telecommunications Law Article 38 - Electronic Transactions Law	Anti-False Content Act (2019) Article 154 - Penal Code	Sections 14 to 17 - Computer Crime Act (2007) Regulation on Prevention, Suppression, and Solving Problems of Fake News Dissemination on Social Media (2022)	Protection from Online Falsehoods and Manipulation Act (POFMA) (2019) Online Safety (Miscellaneous Amendments) Act (2022)	Cybersecurity Law (2018) Article 117 - Penal Code Decree No. 15/2020/ND-CP
ISPS, media, and tech companies	Printing and Publishing Law (2014) News Media Law (2014) Cyber Security Law (2022) Broadcasting Act (2021)	Public Telecommunications Policy Act (1994) Freedom of Information Order (2016)	Broadcasting and Television Business Act (2008) New Ministerial Regulation of MDES (2021) The Notice Procedure, the Suppression of Dissemination of Computer Data and the Deletion of Computer Data from the System B.E. 2565 (2022)	Newspapers and Printing Presses Act (1974) Broadcasting Act (1994) Public Order and Safety (Special Powers) Act (2018)	Press Law (1989) Publication Law (No. 30/2004/QH11) Telecommunications Law (No. 41/2009/QH12) Decree No. 97 (No. 97/2008/ND-CP) Decree 15/2020/ND-CP Decree No. 53/2022/ND-CP
Mass surveillance	Law Protecting the Privacy and Security of Citizens (2017) Telecommunications Law (2013)	SIM Card Registration Act (2022)	Cybersecurity Act (2019) National Intelligence Act (2019)	Cybersecurity Act (2018)	Decree Number 72/2013/ND-CP
Covid-19 temporary and emergency laws, regulations, task forces.	Section 27 - Natural Disaster Management Law (2020) Central Committee on Prevention, Control and Treatment of COVID-19 (Task Force, March 2020)	Bayanihan to Heal as One Act (2020) replaced by the Bayanihan to Recover as One Act (2020) Inter-Agency Task Force for the Management of Emerging Infectious Diseases (Task Force, January 2020) StaySafePH & COVID-KAYA (Tracking Devices, May 2020)	Emergency Decree on Public Administration in Emergency Situations (2005) COVID-19 Emergency Decree (2020) Center for COVID-19 Situation Administration (Task Force, March 2020) COVID-19 Fake News Center (Fake News Task Force, May 2021) ThaiChana & MorChana (Tracking Devices, May 2020)	COVID (Temporary Measures) Act (2020) Multi-Ministry Taskforce on COVID-19 (Task Force, January 2020) TraceTogether (Tracking Device, March 2020)	Sections 5 to 9 & 27 Emergency Decree on Public Administration in Emergency Situation (2005) Decree 15/2020/ND-CP National Steering Committee for COVID-19 Prevention and Control (Task Force, January 2020) Bluezone & NCOVI (Tracking Device, 2020)



The laws and regulations featured on this table don't belong to a single defined category but can also be placed within other categories. While the list is not exhaustive, it captures the essence of the primary legal frameworks in place.

Fig. F: Key Events Driving Digital Dictatorship in Southeast Asia; see country chapters for timeline visualisations.

Country	Event	Contextualisation
 CAMBODIA	 National Internet Gateway (NIG) Sub-Decree (2020)	This sub-decree was designed to strengthen government control over the Internet by requiring all Internet service providers to route their traffic through a centralised control point, the National Internet Gateway.
	 Law on Measures to Prevent the Spread of COVID-19 and other Severe and Dangerous Contagious Diseases	This law has been particularly used to control the dissemination of certain information deemed sensitive or potentially detrimental to the management of the health crisis.
	 Elections	The legislative elections in Cambodia, held on July 23, 2023, faced significant criticism for taking place in the absence of the main opposition party, the Candlelight Party, which was not allowed to participate. These elections were widely seen as tailored to ensure the victory of the Cambodian People's Party (CPP), led by Prime Minister Hun Sen, as part of an effort to validate the transition of power to Hun Manet, the eldest son of Prime Minister Hun Sen.
	 The Inter-Ministerial Prakas No. 170 on Controlling the Publication of Websites and the Handling of Social Media	This Prakas grants extensive powers to government ministries to monitor online activities, block websites, and censor any content that may be perceived as threatening national security, public order, and social interests. However, it lacks clear definitions, giving authorities broad discretion in its implementation.
 INDONESIA	 Ministerial Regulation Number 5/2020 on Private Electronic System Operators (MR 5/2020)	The regulation gives the Indonesian Ministry of Communications and Information Technology (MoCI) broad powers to block and restrict access to online content deemed inappropriate or harmful, without clearly defining the criteria or procedures for determining what constitutes a violation.
	 New Criminal Code (Law No. 1 of 2023)	The New Criminal Code stipulates harsh penalties for speech-related offenses including the dissemination of false information, insults, defamation, and the promotion of abortion.
	 Presidential Instruction No. 1/PNPS/1965 on the Abuse and Defamation of Religion	This legislation has been used to incorporate a provision on blasphemy into the penal code. It stipulates penalties of up to five years' imprisonment for individuals who deliberately and publicly exhibit sentiments or actions that are derogatory, disrespectful, or offensive towards a religion embraced in Indonesia, with the aim of dissuading others from adhering to any faith centered on belief in the One God.
	 Law on Electronic Information and Transactions (ITE Law)	Despite the Indonesian government's effort to revise the ITE Law, several problematic articles, including those concerning defamation, hate speech, and false news, have systematically hindered the fundamental right to freedom of expression and have silenced advocates for human rights.
 LAO PDR	 Telecom Law (2021)	Telecom Law 2021 requires ISPs to cooperate with the government to block access to certain online content deemed inappropriate or against the law. In addition, Telecom Law 2021 provides for severe penalties, including substantial fines, for ISPs that fail to comply with the requirements of the law.
	 SIM Card Registration Act (2020)	This law requires all SIM card users to register their personal details, including name, address and identity card number, with telecoms operators.
	 Elections	The Laotian legislative elections of 2021 took place on February 21, 2021, to elect members of the 9th legislature of the National Assembly of Laos. Laos is a single-party state, where the Lao People's Revolutionary Party (LPRP) is the only legal party and controls the entire electoral process. Elections in Laos are not considered free and fair, as all candidates are approved by the LPRP, and no significant opposition is allowed.

 MALAYSIA	 The Emergency (Essential Powers) (No. 2) Ordinance	This law has been particularly used to control the dissemination of certain information deemed sensitive or potentially detrimental to the management of the health crisis.
	 Elections (2020)	Muhyiddin Yassin was appointed as the Prime Minister in politically complex circumstances triggered by the sudden resignation of Prime Minister Mahathir Mohamad in February 2020. Subsequently, a political crisis erupted. The manner in which Muhyiddin Yassin became Prime Minister sparked controversies and debates on the legitimacy of the process.
	 Elections (2021)	Ismail Sabri Yaakob was elected as the Prime Minister of Malaysia on August 21, 2021. He assumed office following the resignation of his predecessor due to political pressure. Ismail Sabri was appointed Prime Minister after gaining the support of a majority of members in the Malaysian Parliament, and there were no elections per se. Instead, Ismail Sabri was selected through the internal political process of Parliament, where members expressed their confidence in his ability to form a stable government.
	 Elections (2022)	Anwar Ibrahim became the Prime Minister of Malaysia on November 24, 2022, following legislative elections. His appointment marked the end of a prolonged period of political uncertainty post-elections. The 15th Malaysian General Elections (GE15), the first since the Covid pandemic lockdown, aimed to restore political stability after three different prime ministers since 2018. However, the results were inconclusive, with no single coalition winning the minimum seats to form a government. Subsequently, the King entrusted Anwar Ibrahim with the task of forming a new government.
 MYANMAR	 Cyber Security Law (2022)	This law outlaws the use of Virtual Private Networks (VPNs), infringing upon individuals' right to access information online.
	 Illegitimate coup (2021)	On February 1, 2021, the Burmese military overthrew the civilian government led by Aung San Suu Kyi, ending several years of democratic transition. The military declared a state of emergency, citing allegations of electoral fraud during the November 2020 elections, which were won by Aung San Suu Kyi's party, the National League for Democracy (NLD).
 THE PHILIPPINES	 SIM Card Registration Act (2022)	This law requires all SIM card users to register their personal details, including name, address and identity card number, with telecoms operators
	 Anti-Terrorism Act (2020)	It grants the government broader powers to prevent and combat terrorism, including the authority to conduct warrantless arrests and detain suspects for an extended period without judicial warrant, allowing the designation of individuals or groups as terrorists without due process and grants authorities the power to conduct surveillance.
	 Elections (2022)	Ferdinand Marcos Jr., commonly known as Bongbong Marcos, emerged victorious in the presidential election in the Philippines. The son of the late former President Ferdinand Marcos, who ruled the country as a dictator for over two decades, Marcos Jr.'s win has sparked discussions and reactions given the historical context associated with his family's regime.

 SINGAPORE	 Online Safety (Miscellaneous Amendments) Act (2022)	The law grants extensive authority to block online content as deemed necessary by the government.
	 The Online Criminal Harms Act (2023)	It introduces stricter regulations and penalties for individuals and entities engaged in online criminal activities.
	 Election (2020)	the ruling People's Action Party (PAP), led by Prime Minister Lee Hsien Loong, maintained its uninterrupted hold on power despite a notable decline in popular support. The PAP, in power since 1959, secured a super majority by winning 83 out of 93 seats in parliament. The remaining 10 seats were claimed by the Workers' Party, marking the highest number ever held by opposition lawmakers since Singapore's first general election in 1968. Despite its victory, the PAP's share of the popular vote saw a decline to 61.2%, compared to nearly 70% five years ago and approaching the party's record low of 60% in 2011. The election recorded a high voter turnout of nearly 96%.
 THAILAND	 Regulation on Prevention, Suppression, and Solving Problems of Fake News Dissemination on Social Media (2022)	Many critics fear that this regulation could be used abusively by authorities to censor dissenting opinions and suppress freedom of expression. Some view this measure as an infringement on media freedom and democracy, as it grants authorities extensive powers to control and filter online content.
	 The Notice Procedure, the Suppression of Dissemination of Computer Data and the Deletion of Computer Data from the System B.E. 2565 (2022)	The law empowers authorities to issue notices to internet service providers (ISPs) and online platforms to remove or suppress content deemed illegal or harmful.
	 Elections (2023)	Progressive and pro-democracy opposition parties, notably the Move Forward Party led by Pita Limjaroenrat, secured a significant victory in Thailand's recent elections. This outcome challenges the long-standing dominance of military-backed incumbents, signaling a strong desire for change among Thai voters. The Move Forward Party is projected to win 151 seats, the highest in the House, while the populist Pheu Thai Party is expected to secure 141 seats. Together, they hold at least 292 seats in the 500-member House. However, challenges persist in forming a government due to the military's influence, particularly through the appointed Senate. Move Forward is currently 67 votes short of the majority needed for Pita Limjaroenrat to become prime minister, leaving uncertainties about potential government formation.
 VIETNAM	 Decree 15/2020/NĐ-CP	It criminalises the dissemination of false and misleading information, insulting reputations, damaging moral or social values, and revealing state secrets.
	 Decree No. 53/2022/ND-CP	The decree imposes stricter requirements on internet service providers and social media platforms to monitor and remove content deemed to be harmful or illegal, particularly content related to national security, public order, and social morality.
	 Decree No. 72/2023/ND-CP	The decree imposes stricter requirements on social media companies operating in Vietnam, including the establishment of local representative offices and the appointment of local representatives responsible for compliance with Vietnamese laws. It also mandates that social media platforms must remove content deemed to be illegal or violating Vietnamese laws within 24 hours of receiving a request from competent authorities.
	 Elections (2021)	Luong The Huy and pro-democracy forces scored a surprising victory in Vietnam's May 2021 general elections, dealing a significant blow to military-backed incumbents. The progressive Move Forward Party, led by Pita Limjaroenrat, is projected to win 151 seats, while the populist Pheu Thai is expected to secure 141 seats, collectively holding at least 292 out of 500 seats in the House.
	 Elections (2023)	Vietnam's National Assembly appointed Vo Van Thuong as the new president in a leadership reshuffle amid an anti-graft campaign. Thuong, 52, secured the position with 98.38% of the votes in the largely ceremonial role. His appointment follows the abrupt resignation of his predecessor Nguyen Xuan Phuc in January, linked to alleged "violations and wrongdoing." Thuong, a Politburo member and anti-corruption advocate, pledged to continue the fight against corruption. Seen as close to General Secretary Nguyen Phu Trong, Thuong's election is considered a step towards leadership stability, reassuring investors and signaling continuity in foreign and economic policies.

Chapter V.

Recommendations

Based on the foregoing analysis, we are able to identify primary actors who hold key functions in enhancing the state of digital freedoms in Southeast Asia, specifically that of online expression.

Governments hold the obligation to respect, protect and fulfil those freedoms in accordance with international human rights standards. Members of Parliament, on the other hand, are meant to serve the ASEAN population, by responding to our needs for justice and true democracy. They are principally proxies through which governments can effectively satisfy their role; they are responsible not just for the creation, but also the smooth implementation, of laws and regulations that adhere to existing standards. Furthermore, civil society groups are front and centre in voicing the factual needs of the people, monitoring the development of the situation on the ground and advocating the core demands of a free and democratic digital society. Finally, tech companies, given the increasing relevance of technology to the realisation of human rights in practice, have a responsibility to respect human rights and remedy abuses.

Recommendations to Governments

- 1 Decriminalise defamation and libel and bring any other relevant provisions of the Criminal and Penal Codes into line with article 19 of the International Covenant on Civil and Political Rights;
- 2 Enact a stand-alone anti-SLAPP law to ensure legal protections against strategic lawsuits against public participation (SLAPP) aiming at silencing dissent, and protect individuals from judicial harassment by the state and corporations;
- 3 Repeal or substantially amend laws and regulations that unduly restrict freedom of expression, independent media, and access to information, to bring them in line with international human rights law. In particular, clarify or reform vague laws, so that they are written in ways that are comprehensible and accessible to all members of society, so that all society members are aware of their responsibilities, protections, and the consequences of not abiding. The repeal or amendment process should include effective public consultation (in particular, taking into account historically marginalised opinions);
 - a. Clarify legal responsibility under civil and administrative law for what constitutes ‘online gender-based violence (OGBV),’ ‘hate speech,’ ‘hateful conduct,’ ‘harassment,’ ‘doxxing,’ and other key terms, while simultaneously upholding the right to freedom of expression and opinion. Enable people of marginalised groups (e.g. women, LGBTIQ+, disabled peoples, people marginalised based on race, Indigenous peoples, etc.) to guide and participate in the development of reasonable definitions for terms used in legislation that disproportionately affect them. Ensure that reports of online gender-based violence (OGBV) are subject to systematic and consistent investigation, and offer assistance to individuals or groups affected;
 - b. Expand any definitions of ‘personal information’ and/or ‘private information’ to protect (if not already protected) an individual’s full legal name; date of birth; age; gender/legal sex; LGBTIQ+ identity; places of residence, education and work; private personal information of family members and relatives; descriptions and pictures depicting an individual’s physical appearance; and screenshots of text messages or messages from other platforms. These should be considered when investigating cases of doxxing, smear campaigns, and other instances of online violence that weaponise an individual’s personal/private information

against them. Ensure that reports of doxxing campaigns and other forms of violence on the digital space are subject to systematic and consistent investigation, and offer assistance to individuals or groups affected.

- 4 When punishing expression as a threat to national security under laws, the government must demonstrate, with evidence, that:
 - a. the expression is intended to incite imminent violence;
 - b. it is likely to incite such violence; and
 - c. there is a direct and immediate connection between the expression and the likelihood of occurrence of such violence, in line with the Johannesburg principles;¹
- 5 Guarantee transparency and access to information, both offline and online, particularly where such information relates to the public interest and impacts upon the individual's right to public participation, including by amending existing laws or adopting a law to enable provision of such access. Implement measures to enhance transparency in political advertising, including clear disclosure of funding sources and target audiences to promote accountability and integrity, and combat disinformation;
- 6 Enable HRDs, journalists, civil society members, ordinary users, lawyers and academics to safely carry out their legitimate online activities to spread awareness for human rights violations without fear or undue hindrance, obstruction, judicial harassment, and/or online harassment (e.g. OGBV and general OBV, hate speech campaigns, or doxxing);
- 7 Working with responsible MPs and with tech companies, enforce social media policies to prevent harmful effects of doxxing, while considering applicable regulations in relevant countries. Establish a committee, if not already in place, to ensure compliance with these regulations, with a particular focus on moderating or removing illicit content.
- 8 Repeal or amend all laws and regulations that establish a licensing regime for the print and online media, replacing them with a system of self-regulation;
- 9 Cease the targeting and criminalisation of legitimate online speech by opposition activists, journalists, HRDs, and other dissenting voices solely in the exercise of their rights to free expression online, through the abuse of laws and administrative regulations;
- 10 Prevent acts of harassment and intimidation against, the placement of arbitrary restrictions on, or arrests of journalists, activists and human rights defenders who merely criticise public officials or government policies;
- 11 Recognise online and technology facilitated online gender-based violence (OGBV) as a human rights violation and include it in laws to criminalise and prohibit all forms of violence in digital contexts. Enhance the capabilities of law enforcement agencies to effectively investigate and prosecute such crimes;
- 12 Strengthen collaboration with the technology industry, feminist organisations, civil society, and national and regional human rights bodies to bolster measures and policies aimed at promptly and effectively providing remedies to victims of online gender-based violence (OGBV);
- 13 Implement an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards are put in place to regulate such practices. In cases where such technologies have been deployed, ensure both targeted individuals and non-targeted individuals whose data was accessed as a result of someone else's surveillance are notified, implement independent oversight, and ensure targets have access to meaningful legal remedies;

1. ARTICLE 19, *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, (November 1996), available at: <https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>

- 14 End all legal proceedings against individuals facing investigation, charges or prosecution initiated by state authorities for engaging in legitimate activities protected by international human rights law or for addressing violations. Cease all violence against independent media and journalists allowing them to freely report on the emerging situation in the country and stop all efforts to restrict independent information from reaching people;
- 15 Legally recognise human rights defenders and provide effective protection to journalists, HRDs and other civil society actors who are subjected to intimidation and attacks owing to their professional activities;
- 16 Ensure that all measures restricting human rights that may be taken in response to mass-destabilising events, including public health emergencies such as a global pandemic, are lawful, necessary, proportionate and non-discriminatory. Review the measures taken in response to the pandemic in order to ensure that a clear and sufficient legal framework exists for the response to any future pandemic, and take a cautious, progressive approach to emergency measures, adopting those that require derogation only as a last resort when strictly required because other, less restrictive options prove inadequate;
- 17 Take immediate steps to ensure and protect the full independence and impartiality of the judiciary and guarantee that it is free to operate without pressure and interference from the executive;
- 18 Facilitate the participation, leadership, and engagement of a diverse range of people of marginalised communities in government. Create task forces to take proactive initiatives to safeguard marginalised communities (e.g. women, LGBTIQ+, people marginalised based on race) from specific forms of abuse, (e.g. hate crimes, smear campaigns, the sharing of intimate images online including revenge porn), doxxing, hate speech, and overall gender-based violence.
- 19 Carry out routine assessments of the state of digital rights under the jurisdiction. Facilitate the creation of task forces, consisting of individuals trained in the safeguarding of digital rights, to investigate these affairs.
- 20 Set up accessible and appropriate, judicial and non-judicial grievance mechanisms; Provide, among the remedies, fair treatment, just compensation or satisfaction, and the establishment of sufficient grounds to avoid its repetition. Also, implement an evaluation system that regularly screens the existing mechanisms.

Recommendations to Members of Parliament

- 1 Propose amendments to the Criminal and Penal Codes and other laws to address all shortcomings in line with international human rights standards such as UDHR and the ICCPR; and gather consensus among other MPs to ensure these amendments are adopted into the text of the law;
- 2 Hold the government accountable by ensuring that the steps taken by government bodies and agencies in the legal framework are evaluated and analysed on an individual as well as regular basis, applied only in cases where there is a risk of serious harm and cover both the enterprises in the public and private sector without discrimination, particularly when such a step could result in the violation of rights of individuals affected;

- 3 Build discussion and debate around digital rights with specific attention paid to the country context as well as good practices adopted regionally and internationally, with the general public actively involved in providing the grassroots perspective;
- 4 Adopt and enforce national laws to address and punish all forms of gender based-violence, including in the digital space. Legal and policy measures to eradicate online gender-based violence (OGBV) should be framed within the broader framework of human rights that addresses the structural discrimination, violence and inequalities that women and other communities marginalised based on gender (e.g. the LGBTIQ+ community) face. Policies should also highlight specific forms of abuse that people marginalised based on gender often face online (e.g. doxxing, non-consensual sharing of intimate pictures online, the spread of deep fakes);
- 5 Adopt specific laws and measures to prohibit new emerging forms of online gender-based violence (OGBV), as well as specialised mechanisms with trained and skilled personnel to confront and eliminate online gender-based violence;
- 6 Organise and take responsibility for task forces that will take proactive initiatives to safeguard marginalised communities (e.g. women, LGBTIQ+, people marginalised based on race) against specific forms of abuse (e.g. hate crimes, smear campaigns, the sharing of intimate images online including revenge porn), doxxing, hate speech, and overall gender-based violence.
- 7 Ensure that the opposition parties are allowed to fully participate in drafting and passing legislation to enable them to fully represent their constituents.

Recommendations to Tech Companies

- 1 Ensure the companies' terms of services and policies are uniform and in compliance with international standards on freedom of expression, which are reviewed regularly to ensure all circumstances and situations that may arise have been addressed, while also addressing new legal, technological, and societal developments, in line with the obligation to respect human rights under the UNGPs;
- 2 Drop the for-profit business model that revolves around overcollection of data. Such business models are being utilised by the government and are violating data rights.
- 3 Adopt the Global Network Initiative Principles on Freedom of Expression and Privacy;
- 4 Clearly and completely explain in guidelines, community standards, and terms of services what speech is not permissible, what aims restrictions serve, and how content is assessed for violations;
- 5 Ensure the integrity of services by taking proactive steps to counteract manipulative tactics utilised in the dissemination of disinformation, including the creation of fake accounts, amplification through bots, impersonation, and the proliferation of harmful deep fakes.
- 6 Prioritise prediction of, preparation for, as well as protection against digital dictatorship and online-based violence when launching, revolutionising, or reforming products, services, and initiatives. The guidelines of the Center for Countering Digital Hate

(CCDH) 'STAR Framework' should be urgently considered, which include: safety by design; transparency in algorithms, rules enforcement, and economics; accountability systems implementation; and corporate responsibility.² In addition, these predictive, preparative, and protective factors must take into account and implement the input of marginalised communities (e.g. LGBTIQ+ peoples, women, and those marginalised based on race) who often become targets of online violence that is often unregulated or even perpetuated by existing systems;

- 7 Products, services, and initiatives must have consumer safety in mind from the very beginning of conception. This means that product, service, and initiative developers, as well as high-level executives, must all take all possible measures to ensure that their products are safe, by design for all users, including marginalised communities (e.g. including LGBTIQ+ peoples, women, and those marginalised based on race). Not only does far-sighted consideration ensure user safety and the safeguarding of human rights, but it will also increase the longevity of these products, services, and initiatives in a rapidly changing economy where people are becoming increasingly aware and adamant about the protection of their human rights. Ensuring safety by design includes the practice of performing thorough risk assessments, and educating developers as well as executives to recognise their responsibilities to uphold human rights standards during the development as well as execution processes;
- 8 Promote transparency. CCDH specifically highlights the need for transparency in "algorithms; rules enforcement; and economics, specifically related to advertising." Though transparency is more of a 'preparative' factor rather than a 'preventive' one, it will make civic engagement and corporate accountability much more effective, ultimately amounting to increased 'prevention' efficacy;

- a. Transparency in algorithmic development, for example, is essential; though algorithms are not responsible humans, they were created by responsible humans. This same logic can be applied to Artificial Intelligence (AI); though AI is not human, it was created by humans. If algorithms and AI are developed and/or trained by humans with harmful biases (e.g. misogynistic, anti-LGBTIQ+, ableist, racist biases), they are accordingly likely to cause and perpetuate harm (e.g. misogynistic, anti-LGBTIQ+, ableist, racist harm). Transparency in the development of algorithms, AI, and other technologies is essential so that any harm being perpetuated by these non-human systems can be flagged, and accordingly addressed.
 - b. The same logic can be applied to company regulation development processes, as well as advertising strategy. For example, if company regulations were formulated in a way that disproportionately excludes marginalised voices (e.g without any adopted input from a diverse range of people of intersectional identities, such as women, LGBTIQ+ people, disabled people, or people marginalised based on race), those regulations are more likely to cause or perpetuate human rights violations. Companies should implement measures to enhance transparency in advertising, including clear disclosure of funding sources and target audiences to promote accountability and integrity, and combat disinformation;
- 9 Transparency goes hand-in-hand with effective corporate regulatory and accountability systems. The people who run and work for tech companies, like consumers, are humans, who must be proportionately held accountable for their actions if they intend to create products, services, and initiatives for consumption by civil society. Companies and their stakeholders (particularly senior

2. CCDH, *PUBLIC SUPPORT FOR SOCIAL MEDIA REFORM: Assessing CCDH's STAR Framework for social media regulation, (16 August 2023)*, available at: <https://counterhate.com/research/public-support-for-social-media-reform-star/>; The following recommendations will elaborate on this.

executives) must recognise they hold a lot of economic, political, and social power by virtue of being in their positions, and thus naturally hold more responsibility than the average consumer. This means that though consumers have their own responsibilities, companies cannot put responsibility disproportionately on the consumer to regulate their own use of the companies' products, services, and initiatives, if these companies genuinely intend to safeguard human rights. Thus, companies must implement regulatory systems that put people above profit, in order to allow themselves to be held accountable, and in order to facilitate their self-regulation;

- 10 Enable people of marginalised groups (e.g. women, girls, LGBTIQ+ people, disabled people, people marginalised based on race), to participate and lead in the technology sector to guide the design, implementation, and use of safe and secure digital tools and platforms.
- 11 Commit to eradicating online gender-based violence (OGBV) and allocate resources to information and education campaigns aimed at preventing ICT-facilitated gender-based violence. Additionally, invest in raising awareness for the intersection between human rights and digital security, demonstrating how human rights must be taken seriously in both the offline and online spaces. This can come in many forms, including working closely with local communities and human rights organisations (e.g. feminist groups, LGBTIQ+ groups) to facilitate dialogue and sensitivity training regarding the needs of people marginalised based on gender and/or other factors;
- 12 Implement and communicate stringent user codes of conduct across their platforms, ensuring their enforcement. Additionally, establish uniform content moderation standards that can effectively identify and address nuanced forms of online violence, while remaining sensitive to diverse cultural and linguistic contexts;
- 13 Improve the systems for reporting abuse so that victims of online gender-based violence (OGBV) and racial discrimination can easily report it and track the progress of the reports;
- 14 Publish regular information on official websites regarding the legal basis of requests made by governments and other third parties and regarding the content or accounts restricted or removed under the company's own policies and community guidelines, and establish clear, comprehensive grievance mechanisms that allow governing bodies and civil society members to dispute restrictions or removals of content and accounts. Aside from being clear and comprehensive, these mechanisms must have efficient, effective, and bias-trained systems of humans and/or electronic systems ready to receive and handle the grievances.;
- 15 When appropriate, consider less-invasive alternatives to content removal, such as demotion of content, labelling, fact-checking, promoting more authoritative sources, and implementing design changes that improve civic discussions;
- 16 Engage in continuous dialogue with civil society to understand the human rights impacts of current and potential sanctions, and avoid overcompliance in policy and practice;
- 17 Ensure that the results of human rights impact assessments and public consultations are made public;
- 18 Ensure that any requests, orders and commands to remove content must be based on validly enacted law, subject to external and independent oversight, and demonstrates a necessary as well as proportionate means to achieve one or more aims.
- 19 Organise task forces and initiate proactive initiatives to safeguard LGBTIQ+, women, girls and other concerned minorities against specific forms of abuse, (e.g. the non-consensual sharing of intimate images, including revenge porn), doxxing, hate speech, and overall gender-based violence.

- 20 Carry out routine assessments of human rights impacts and provide comprehensive transparency reports on measures taken to address the against marginalised communities (e.g. e.g. hate crimes, smear campaigns, the sharing of intimate images online including revenge porn).
- 21 Conduct assessments and due diligence processes to determine the impact of business activities on users, with respect to online freedom. Ensure meaningful and inclusive stakeholder engagement, with no one left behind.

Recommendations to Civil Society

- 1 Set up an independent multi-stakeholder body with the cooperation of various sectors to monitor and provide recommendations on trends in, and individual cases of digital rights abuses;
- 2 Work alongside governments and other stakeholders, to generate dialogue on issues and ensure accountability of government measures especially when it comes to issues related to democracy and human rights;
- 3 Support the independent evaluation and analysis of substantive aspects, including the use of the principles of necessity and proportionality through established global standards, and the impact of responses on society and economy;
- 4 Hold implementing authorities and officials liable for the misuse of their powers or information obtained, while carrying out their duties in the existing legal framework;
- 5 Strengthen understanding and solidarity among underprivileged people (e.g. class solidarity, solidarity among women and others marginalised based on gender, understanding among different ethnic groups within a jurisdiction);
- 6 Promote a safe and respectful environment for free online expression;
- 7 Continue to increase knowledge on digital security through training and capacity building programs, and actively carry out training on media literacy, including how to verify information to be true;
- 8 Continue to conduct awareness campaigns to educate individuals and communities about the various forms of gender-based violence, its impact on survivors, and the importance of promoting a safe and respectful online environment;
- 9 Advocate for the implementation and enforcement of robust laws and policies that criminalise all forms of gender-based violence, including online gender-based violence (OGBV);
- 10 Develop and implement digital literacy programs that equip individuals, especially women and marginalised communities, with skills to navigate online platforms safely, recognise and respond to online harassment, and protect their privacy;
- 11 Create and participate in grassroots, community-led initiatives to safeguard LGBTIQ+, women, girls and other concerned minorities against specific forms of abuse (e.g. the non-consensual sharing of intimate images, including revenge porn), doxxing, hate speech, and overall gender-based violence. Wherever possible, mobilise these initiatives to hold governments, MPs, and corporations accountable.
- 12 Collaborate with social media platforms and technology companies to develop and enforce policies and mechanisms that effectively address online gender-based violence (OGBV).

Glossary

Abolition: putting an end to something by law

Appeal: the resort to a higher court to review the decision of a lower court, or to a court to review the order of an administrative agency

Arresto mayor: In Philippine criminal law, a sentence of imprisonment with a full range of one month and a day to six months

Attorney: a person legally appointed or empowered to act on behalf of another person

Bail: a sum of money paid by a defendant upon release to ensure later appearance in court

Bill: a statute in draft, before it becomes law

Charge: the specific statement of the crime accused to a party in the indictment or criminal complaint in a criminal case

Chilling effect: suppression of free speech and legitimate forms of dissent among a population due to fear of repercussion

Customary international law: international obligations arising from established international practices accepted as the norm

Conviction: an adjudication or formal declaration of a criminal defendant's guilt

Damages: a sum of money the law imposes to compensate a loss or injury

Defendant: someone who is being sued or accused of committing a crime

Distributed Denial-of-Service (DDoS) attack: a malicious attempt to disrupt normal traffic to a website or targeted server

De facto: Latin for "in fact." Phrase to show that that a state of affairs is true in fact, but not officially sanctioned

Directive: a set of instructions, guidelines, decisions or regulations issued by an official body outlining how a legal objective is to be achieved

Disenfranchisement: the removal of the rights and privileges inherent in an individual or group

Doxxing: publicly revealing identifying information about a person online

Entry into force: the coming into effect of a law or international agreement as to make it binding

Extradition: surrender by a country of a person charged with a crime in another country, usually under provisions of a treaty

Felony: a crime, characterised under federal law and state statutes as any offence punishable by imprisonment of over one year or death

Grievance mechanism: a formalised process, either judicial or non-judicial, by which a harm or cost suffered by a person can be compensated or remedied

Hoax: a trick or something else that is intended to deceive someone

Incommunicado detention: a situation of detention where a person is denied access to family members, an attorney or independent physician

Indictment: a formal written accusation stating that a person is being charged with a crime and must undergo a criminal trial

Injunction: a court order by which a person is ordered to perform, or restrain from performing, a certain act

Lawsuit: a disagreement between people or organisations that is brought to a court of law for a decision

Libel: a published false statement that is damaging to a person's reputation

Moratorium: a delay or suspension of an activity or law until further consideration

Perjury: the intentional act of swearing a false oath or falsifying an affirmation to tell the truth, whether spoken or in writing, concerning matters material to an official proceeding

Persecution: severe discrimination that results in the denial or infringement of fundamental rights

Phishing: a technique to trick a person into disclosing sensitive data through the use of deceptive emails or websites

Pre-trial detention: the detaining of an accused person in a criminal case before the trial has taken place

Prisión correccional: In Philippine criminal law, a sentence of imprisonment with a full range of six months and one day to six years

Prisión mayor: In Philippine criminal law, a sentence of major imprisonment with a full range of from six years and one day to twelve years

Probation: an alternative to imprisonment allowing a convicted person to stay in the community, usually under conditions and supervision of a probation officer

Prosecution: the initiation of criminal proceedings against a person accused of a crime

Ratification: an international act whereby a state expresses its consent to be bound to a treaty by an exchange or deposit of requisite instruments

Redress: relief or remedy or a means of seeking relief or remedy

Red-tagging: a harmful practice that targets people who often end up being harassed or even killed

Reverse onus: a legal provision that shifts the burden of proof onto a specified individual, normally the defendant, to disprove an element of an information

Self-censorship: withholding of one's true opinion from others in the absence of formal obstacles

Slander: false oral statements which damages the reputation of others

SLAPP suit: a civil claim filed against an individual or organisation to dissuade criticism, or intimidate or harass into silence

Smear campaign: a planned attempt to harm the reputation of a person or company by telling lies about them

Status quo: state of affairs as it exists at a particular time, normally one that precedes a controversy

Statute of limitations: a law that sets the maximum time that parties have to initiate legal proceedings from the date of an alleged offence

Sub judice contempt: a form of law that protects a person's right to a fair hearing by preventing the publication of material or comment which may improperly influence a jury or witness

Summons: a document issued by a court notifying someone that they are being sued or required to appear in court

Uphold (of a decision): to agree with a decision made earlier by a lower court

Writ: a written order issued by an administrative or judicial body

#STOPDIGITAL DICTATORSHIP

