ASEAN PARLIAMENTARIANS FOR HUMAN RIGHTS

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

PROMOTING INTERNET FREEDOMS IN SOUTHEAST ASIA

Toolkit for Parliamentarians

Purpose of the toolkit

This toolkit aims to empower parliamentarians (MPs) to advocate for internet freedoms by introducing international norms and standards governing it, highlighting common and pressing challenges, and identifying avenues and recommendations on how MPs can utilize their role to promote and strengthen these freedoms.

The COVID-19 pandemic has reinforced the role of the Internet as a basic necessity, indispensable to conducting work, attending school, and participating in social and political activities. In January 2021, around 59.5 % of the world's population was using the Internet, 10% of which is in Southeast Asia. The United Nations and many governments around the world have also recognized internet access as a human right, the fulfillment of which relies on the safe and free exercise of Internet freedoms.

As the Internet continuously grows, it has also become a **battleground for human rights**, with state and non-state actors using it to either put people at risk of human rights abuses or prevent individuals from fully and safely exercising their Internet freedoms.

WHAT ARE INTERNET FREEDOMS?

Internet freedoms, or digital rights, refer to the exercise of people's human rights online.

The UN clearly stated that **"the same rights that people have offline must be protected online."** This means that all the rights enshrined in the International Covenant on Civil and Political Rights (ICCPR) apply online, including the **rights to freedom of expression, association, and peaceful assembly** and the **rights to access to information and to privacy.**

While these rights – whether exercised online or offline - are not absolute, governments can only restrict these rights in limited ways and only in certain circumstances. Specifically, as enshrined in the ICCPR, any restrictions to these rights must be provided by law and be based on necessity for the respect of the rights or reputation of others; for the protection of national security or of public order, or of public health or morals.

What are the international standards governing internet freedom?

The international human rights framework governing internet freedom is also based on existing frameworks governing freedoms offline. As the United Nations Human Rights Committee declared in a resolution in July 2021 that **"the same rights that people have offline must also be protected online."**

Internet freedoms are founded on foundational rights that enable other rights to be exercised such as **the freedom of expression, freedom of association, freedom of peaceful assembly, and the right to privacy**. These rights are expressed in the UN Declaration of Human Rights (UDHR) and protected in a legal treaty through the International Covenant on Civil and Political Rights (ICCPR).

Freedom of Expression (Article 19): Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Freedom of Association (Article 22): Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.

Freedom of Peaceful Assembly (Article 21): The right of peaceful assembly shall be recognized.

Right to Privacy (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 honor and reputation.

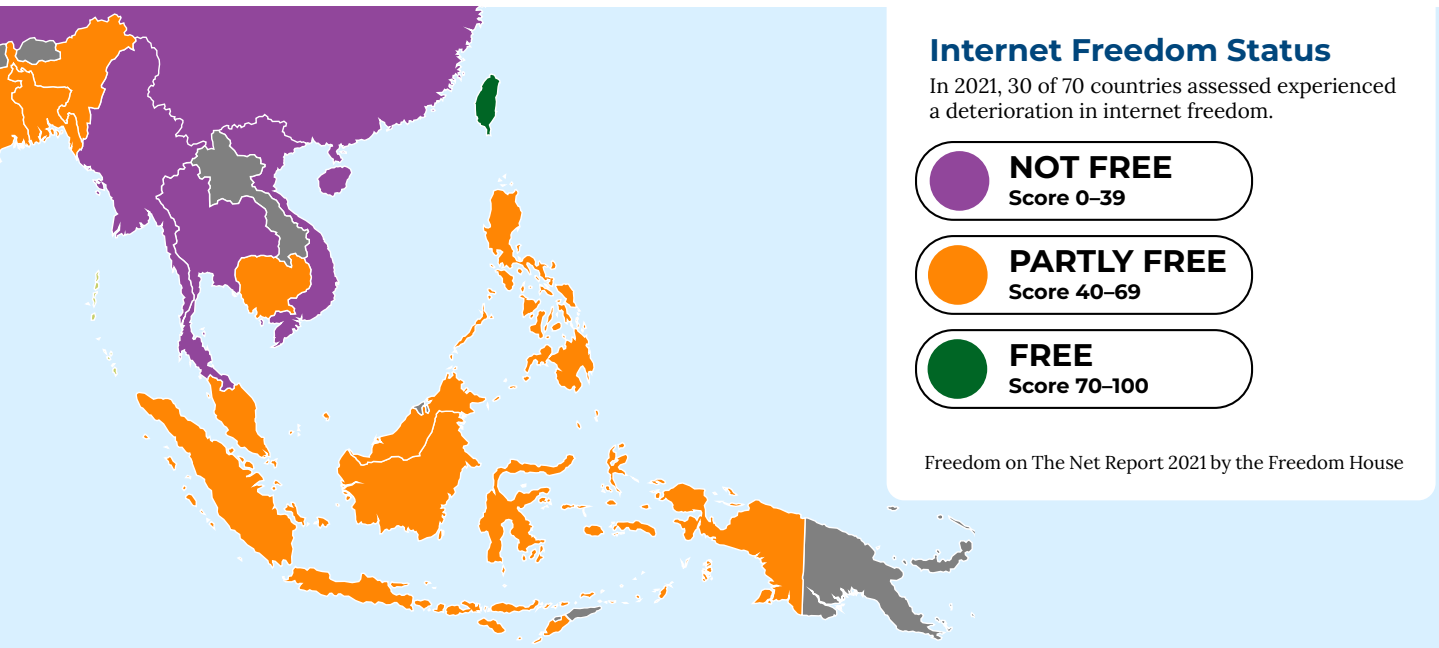
While freedom of expression is not an absolute freedom, any restrictions shall respect Article 19 of the ICCPR, any restrictions should be **provided by law** and are **based on necessity**, for respect of the rights or reputation of others and for the protection of national security or of public order, or of public health or morals. Any restrictions must comply with Article-19's three-part test.

ARTICLE 19'S THREE-PART TEST:

- The restriction must be provided by law, which is clear and accessible to everyone;
- The restriction must pursue one of the legitimate purposes in Article 19(3), namely: to protect the rights or reputations of others; to protect national security or public order, or public health or morals;
- The restriction must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

HOW ARE INTERNET FREEDOMS RESTRICTED?

In the 2021 Freedom on the Net report which measures ways our rights are restricted online, no country in Southeast Asia was considered "*free*" with the majority only qualifying as "*partly free*" and Myanmar, Thailand, and Vietnam rated as "*not free*." The common challenges found in the region are the restricted and limited access to the internet, online disinformation, hate speech, censorship and attacks on online critics, data protection and violations to the right to privacy, and online gender-based violence.



Restricted & limited access to the Internet

Intentional disruption of Internet access is a human rights violation and States should adopt national policies towards its universal access. Not having access to it exacerbates socio-economic inequalities, undermines democracy, and prevents the full exercise of Internet freedoms.

Limitations in access can be due to **infrastructure or economic factors**. In Southeast Asia, Brunei ranks highest in Internet penetration with 97.5% reach among its population, followed by Malaysia and Singapore. **Many countries, however, still cannot afford expansive and stable Internet connection**. Timor Leste only records 30.5% of Internet penetration and subscribers experience slow Internet speeds and expensive subscription rates.

Another major obstacle to Internet access can result from **governments intentionally blocking websites and social media platforms, slowing access or throttling connection speeds, or imposing full or partial** Internet shutdowns, often to control the flow of information, silence protests, sway elections, or hide human rights violations. These shutdowns can also have negative consequences on the economy, education, and health care.

In the first five months of 2021, 50 internet shutdowns in 21 countries worldwide were documented including those imposed by **Myanmar's** military at various times and in different regions since the February coup. In 2019 and April 2021, the **Indonesian** government ordered Internet services to be disconnected to obstruct information flow in West Papua as protests and conflicts escalated.

Online disinformation

Disinformation is information that is false and shared with the intention to mislead or deceive a population. While the practice is not new, it has become more pervasive in the digital age. It can be perpetuated by states, politicians, political parties, businesses, and other powerful individuals supported by "troll armies" (organized groups of people disseminating false information or propaganda in the Internet and social media platforms) or public relations companies.

The spread of disinformation poses serious threats to human rights and democracy. It can compromise the integrity of electoral processes; threaten people's right to health; facilitate discrimination; prompt attacks against people's honor and reputation; or create the potential for physical violence and conflict.

In Thailand and the **Philippines**, entities directly related to the authorities have been linked to organized disinformation campaigns against opposition lawmakers and human rights activists to undermine and threaten them. In 2019, Facebook removed at least 200 pages of coordinated inauthentic behavior that were linked to a network organized by the social media manager of President Duterte's electoral campaign.

Online Hate Speech

Hate speech refers to all forms of expression that attacks or uses pejorative or discriminatory language on the basis of who a person or a group of persons are: their religion, ethnicity, nationality, race, color, descent, gender, or other identity factor. It is prohibited only when it takes the form of **incitement** to discrimination, hostility, and violence.

Because of the speed and reach of the Internet, the impact of hate speech online can be disastrous, resulting in: large-scale violence and atrocities; gender-based violence; violent extremism; discrimination; and racism. It threatens democratic values, social stability, and peace.

Article 20(2) of ICCPR specifically states that "any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility or violence, shall be prohibited by law."

In **Myanmar** social media was widely used to spread hate and discrimination against the Rohingya minority ahead of the mass atrocities perpetrated against them by the military in 2017. Reuters found 1,000 examples of posts, comments, and pornographic images on Facebook attacking and inciting violence against the Rohingya and other Muslims.

During the COVID-19 pandemic in Malaysia, hate speech filled Facebook pages targeting Rohingya refugees. Reuters found dozens of pages, groups, and accounts run by former and serving Malaysian security officials encouraging violence. This led to instances of physical assaults of refugees and for some to lose their livelihood.

Censorship and attacks of online critics

The power of expression on the Internet, especially on social media platforms, has become a threat to undemocratic governments. Often in the name of combating cybercrime, disinformation, or hate speech, governments adopt vague laws and regulations to block content or criminalize expression online they deem too critical.

In **Vietnam**, the 2019 Cybersecurity Law gives sweeping powers to authorities to censor blogs and social media platforms. Internet service providers who publish banned content can be fined or face closure. Amnesty International found 69 prisoners of conscience imprisoned for expressing opinions on online platforms in 2020.

In **Singapore** the 2019 Protection from Online Falsehoods and Manipulation Act (POFMA) allows a single government minister to declare information online as "false" and to order its "correction" or removal. By 2020, the law had been invoked more than 50 times, mostly against people or publications that criticized the government.

In **Cambodia** the government prosecuted individuals who criticized its handling of the COVID-19 pandemic online including a journalist for a Facebook comment and at least three individuals for posting TikTok videos criticizing the use of Chinese-made vaccines.

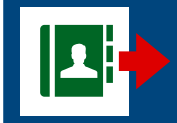
In **Thailand** the authorities repeatedly used the Computer-Related Crime Act (CCA) to arrest members of the pro-democracy protests. Between July 2020 and September 2021, 90 people in 103 cases were charged under the CCA.

Data protection and violations of the right to privacy

The right to privacy protects people from being subjected to arbitrary interference with their privacy, family, home, or correspondence. It is an essential component to the exercise of the right to freedom of expression, especially online. It allows people to express themselves without fear of intrusion or threat to their well-being.

The Internet presents major threats to our right to privacy: Governments and business enterprises **collect and use vast amounts of data** related to the private lives of individuals without their knowledge or without them being aware how this data will be used. States are reportedly also increasingly conducting mass surveillance and intercepting communications in secret.

Data is collected through computers, smartphones, smartwatches, the use of social media, online banking, e-commerce, or contact tracing applications during the COVID-19 pandemic.



In **Thailand**, a new set of rules to the CCA released in August 2021 instruct digital service providers to collect users' data and hand them over to authorities upon request. Even public venues providing Internet access are required to install surveillance cameras to aid authorities in identifying Internet users.

In **Cambodia**, a sub-decree requires all Internet traffic to be routed through a new National Internet Gateway which monitors online activity before it reaches users. It allows for "blocking and disconnecting [of] all network connections" for things as broadly defined as "safety, national revenue, social order, dignity, culture, tradition and customs." It essentially allows the government to increase online surveillance, censorship, and control of the Internet

Online gender-based violence

Women, girls, and LGBTQ+ are disproportionately impacted **by online violence** through misogynist comments or gender based-hate speech, identity theft, unsolicited nude images, distribution of non-consensual sexually explicit content, online stalking, online threat of violence, sexually charged attacks relating to women's private's lives or their physical appearance, etc.

These attacks online against women increased during the COVID-19 pandemic. They also affect female parliamentarians which threatens women's participation in politics and discredits female politicians.

WHAT CAN PARLIAMENTARIANS DO?

Ensure access and better connectivity for everyone

- ☑ Adopt laws and budget to accelerate the building of infrastructure, especially in underserved populations, and to allow diversity in Internet service providers to encourage competition and fair and affordable pricing and connectivity speeds;

- ☑ Ensure any legal framework referring to Internet shutdowns is in line with international human rights law and meet the requirements of legitimacy, necessity, and proportionality; and

- ☑ Publicly denounce all forms of Internet shutdowns and exercise oversight over your government if it does impose any.

In Malaysia, in its effort to bridge the digital divide, the government in 2018 managed to reduce more than 30% of the broadband prices following the introduction of a Mandatory Standard on Access Pricing policy from the Ministry of Communications and Multimedia. A longer-term plan was later adopted, the National Fiberization and Connectivity Plan 2019-2023 (NFCP) with the aim of improving internet quality and coverage and providing access across all spectrums of society.

Protect people from disinformation and hate speech

- ☑ Ensure that all restrictions aimed at tackling disinformation and hate speech comply with international human rights law and standards, specifically that they are provided for by law, they serve one of the legitimate interests recognized in international law, and are necessary and proportionate to that interest.

A Joint Declaration on Freedom of Expression and "Fake News," Disinformation, and Propaganda issued by the UN and regional human rights bodies in 2017, it stated that "general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news"... are incompatible with international standards for restrictions on freedom of expression" and "criminal defamation laws are unduly restrictive and should be abolished."

The UN developed the **UN Rabat Plan of Action** to be used as a guide when developing legislation related to hate speech. It suggested a high threshold for defining restrictions on freedom of expression, incitement to hatred, and for the application of article 20 of the ICCPR. It outlines a six-part threshold test taking into account:

(1) the social and political context,
(2) status of the speaker,
(3) intent to incite the audience against a target group,
(4) content and form of the speech,
(5) extent of its dissemination, and
(6) likelihood of harm, including imminence.

- ☑ Speak out firmly and promptly against intolerance, discriminatory stereotyping, and instances of hate speech and support dialogues to foster intercultural and interreligious understanding and learning;
- ☑ When possible, collaborate and engage with independent fact-checking organizations to combat disinformation.
- ☑ Support empowerment and education programs for Internet users to capacitate them in identifying false information.

Social media giant, Facebook (now Meta), has a fact-checking program involving independent, third-party organizations in countries around the world. One of the organizations they work with is AFP Fact Check for Malaysia, Indonesia, the Philippines, Singapore, and Thailand. AFP Fact Check takes into account local cultures, languages, and politics and works with AFP's bureaus worldwide to investigate and disprove false information, focusing on items that can be harmful, impactful, and manipulative. Facebook also engages with local fact-checking organizations, such as with Kompas, Mafindo, and Tempor in Indonesia, and Rappler and Vera Files in the Philippines.

In the United States of America (USA), its Congress has proposed the Digital Citizenship and Media Literacy Act to award grants to state and local educational agencies to promote media literacy including the safe, responsible, and ethical use of communication and digital information technology tools and platforms.

Repeal repressive laws, put an end to digital censorship

- ☑ Review, amend, or repeal all repressive laws that infringe on people's fundamental freedoms in consultation with experts and civil society working on human rights. The same should be done to any proposed measure or pending legislation.
- ☑ Call for the immediate and unconditional release of all those currently arbitrarily imprisoned or detained solely for exercising their human rights online.

For the region

- ✓ To repeal Sedition laws, specifically in Brunei and Malaysia that tend to be misused to crackdown on freedom of expression, association, and assembly.
- ✓ To repeal laws that broadly define and criminalize defamation such as in Indonesia's defamation provisions under its penal code and Law on Electronic Information and Transactions and under defamation provisions under Thailand's Criminal Code.

On a National Level

For Cambodia

- ✓ To amend or repeal the new COVID-19 Law that criminalizes or unduly restricts freedom of expression and information.
- ✓ To cancel the sub-decree that established the National Internet Gateway that poses serious risks to freedom of expression and privacy.

For Malaysia

- ✓ To amend or repeal provisions in the Communications and Multimedia Act that allow censorship of content online and target freedom of expression online.

For the Philippines

- ✓ To amend or repeal provisions in the Cybercrime Prevention Act of 2012 that criminalize libel and give authorities unchecked powers to shut down websites and monitor online information.
- ✓ To carefully assess the proposed draft Anti-False Content Law and remove all provisions that undermine democracy, threaten privacy rights, and infringe on people's fundamental freedoms.

For Singapore

- ✓ To amend or repeal the Protection from Online Falsehoods and Manipulation Act (POFMA).

For Thailand

- ✓ To amend or repeal the Cybersecurity Act and Computer-related Crimes Act (CCA), both acts have overbroad provisions and do not provide oversight and accountability mechanisms.

For Timor Leste

- ✓ To strictly scrutinize the draft Cybercrime Laws pending before the parliament to ensure it complies to international laws and standards.

Safeguard people's right to privacy

☑ Adopt robust data privacy legislation that complies with international human rights law by applying the principles of legality, legitimate aim, necessity, and proportionality; and do not impose requirements of blanket, indiscriminate retention of communications data on telecommunications and other companies;

The UN High Commissioner on Human Rights in its 2021 report highlighted that Data privacy frameworks should account for the new threats linked to the use of Artificial Intelligence (AI). As example, "laws could impose limitations on the type of data that may legally be inferred and/or further used and shared. Legislators should also consider strengthening individuals' rights, including by granting them the rights to a meaningful explanation and to object to fully automated decisions that affect their rights..." and "Civil society organizations should be empowered to support enforcement of data privacy laws, including through the establishment of robust complaint mechanisms.

"The General Protection Data Regulation (GPDR) of the European Union, enacted in 2016 and implemented in 25 May 2018, is one of the most comprehensive legislations that regulates the collection and use of personal data by both governments and the private sector. The safeguards provided for in this regulation are very important in this digital age."

- [x] Protect the existence and usage of encryption technologies by ensuring the governments do limit access to anonymity tools.

- [x] Ensure that new surveillance programs meet international human rights standards for necessity, proportionality, and independent oversight; and

> "Encryption and anonymity tools are tools widely used by human rights defenders, civil society, journalists, whistle-blowers, and political dissidents facing persecution. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks. Such a widespread and indiscriminate impact is not compatible with the principle of proportionality.
>
> – The Right to Privacy in the Digital Age, 2018 Report of the UN High Commissioner"

- [x] Establish independent authorities with powers to monitor State and private sector data privacy practices, investigate abuses, receive complaints, and issue penalties for the unlawful processing of personal data.

Support ending gender-based violence

- [x] Refrain from using sexist and abusive language against women and immediately rebuke such comments, including those made by peers;

- [x] Champion policies that eliminate sexism and misogyny, specifically by prohibiting all forms of internet-related violence against women, such as sextortion, live-streaming of sexual abuse, non-consensual dissemination of intimate images.; and
- [x] Support gender and development programs to raise awareness about gender equality and rights, and empower women and other gender minorities on how to protect and defend their rights.

FOR MORE INFORMATION

- 2016 UN General Assembly Resolution on the Promotion, Protection, and Enjoyment of Human Rights on the Internet
- 2018 UN OHCHR Report on the Right to Privacy in the Digital Age
- 2021 UN OHCHR Report on the Right to Privacy in the Digital Age
- 2021 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression
- Joint Declaration on Freedom of Expression and "Fake News," Disinformation, and Propaganda
- Ending Internet shutdowns: a path forward Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association
- Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia
- Creating a Data Protection Framework: Do's and Don'ts Guide for lawmakers
- Freedom House Policy Recommendations: Internet Freedom
- #KeepitOn campaign: Who is shutting down the internet

ASEAN PARLIAMENTARIANS FOR HUMAN RIGHTS

February 2022

ICNL
INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

Cover Page: Scores of students took to the streets asking to restore internet access in the states of Chin and Rakhine as Myanmar authorities ordered a temporary shutdown of internet data services in some areas of the conflict-torn region. © EPA-EFE

Back Cover: Rakhine University Students hold placards during a protest against the internet shutdown in Sittwe, Rakhine State, Western Myanmar, 22 February 2020.© EPA-EFE

www.aseanmp.org
Facebook / Twitter / Instagram: @ASEANMP