Human rights impacts of new technologies on civic space in South-East Asia

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

While the expansion of internet access and proliferation of digital technologies has created unprecedented opportunities for humankind, including in the spheres of communication, commerce, and advocacy, it has also proliferated on-line harms and provided State and non-state actors with tools for targeting critics and competitors, undermining democratic governance, and shaping public discourse in consequential ways. The COVID-19 pandemic has moved more activity online, developing digital civic space and generating new forms of cooperation across national boundaries. But it has deepened discrimination and inequality and made human rights defenders (HRDs), activists, and journalists more vulnerable to surveillance and attack.

The scale and speed of digital communications combined with the limited capacity of tech companies to manage communications in contexts and languages far away from their headquarters add to the broader challenges. When not addressed, episodes of incitement to discrimination, violence and mass disinformation campaigns have significantly increased the risks experienced by marginalized communities and translated into serious real-world violence. In some contexts, digital tools have also been abused for surveillance and harassment of dissenting voices.

Though these are global phenomena, an examination of online civic space in South-East Asia provides an informative perspective on these challenges, and its diverse communities offer expertise and experience that can inform global debates on risks emerging with technologies and the challenges faced when regulating digital space.

The report, based on information related to recent developments in ten countries in the South-East Asia region (Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Viet Nam), identifies six interrelated trends that summarize key challenges faced by civil society engaging in online space:

- Promotion of or failure to curb the **dissemination of hateful and discriminatory content** and its contribution to self-censorship, exclusion, conflict and instability, and online gender-based violence.

- **Organized and coordinated efforts to threaten and harass HRDs**, journalists, and political opposition through trolling, doxing, spreading of defamatory and false information, and other forms of online hostility.

- **Abuse of digital surveillance technologies** by governments (often with the assistance of private companies) of digital surveillance tools – including spyware, facial recognition, and biometric technologies – that violate rights and the proliferation of specialized surveillance bodies.

- **Restrictive legal and regulatory frameworks.** Promulgation of cybercrime, cybersecurity and other laws that expand state power to monitor, censor and suppress online expression and exercise control over digital technologies and infrastructure without adequate transparency and oversight.

- **Arrests and prosecutions relating to expression online.** The criminal prosecution of diverse forms of online expression and application of disproportionate penalties, frequently justified by reference to legitimate public policy aims (such as pandemic response, national security and addressing disinformation and hate speech).

- **Disruption of communications** by States seeking to suppress dissent or constrain civic space by curtailing internet access through the throttling of bandwidth, blocking Virtual Private Networks (VPNs), distributed denial-of-service (DDoS) attacks, and other forms of internet shutdowns.

Online space often replicates hostilities experienced offline. States, companies and civil society around the world are debating alternatives for improving the regulation of digital space and providing adequate responses to concerns about online attacks against individuals and groups. Policy solutions to these problems require a new level of awareness of the functioning of digital space, transparency, cooperation, gender responsiveness, and commitment to human rights principles by governments and companies. This report, therefore, concludes by offering a set of specific recommendations to address the identified trends in line with international human rights law, and the work of United Nations human rights institutions and experts.

INTRODUCTION

THREATS TO CIVIC SPACE ONLINE IN SOUTH-EAST ASIA

This report by the Office of the United Nations High Commissioner for Human Rights (OHCHR) identifies and examines six trends affecting human rights online in South-East Asia. It raises concerns about how States and companies have sought to manage, and in some cases misuse, online space and digital technologies. The report is based on interviews and desk research, including government statements and documents, reports by United Nations Special Procedures and other international bodies, civil society and academic reports, and publicly available data from private sector entities including social media companies. It is grounded in the principles and approaches set out in the United Nations Guidance Note on the Protection and Promotion of Civic Space.[1]

In South-East Asia, as elsewhere in the world, the rapid expansion of digitally enabled communications has brought about a number of new challenges: The spread of incitement, organized online campaigns targeting civil society actors and the rapid expansion of surveillance have increased the challenges faced by those engaging in public debates.

As governments and companies have sought to identify responses to these challenges, they have too often failed to adequately address the complexities. Governments have rapidly introduced regulatory instruments and invested in surveillance capacities, increasing risks of arbitrary and disproportional restrictions to freedom of expression and privacy in the region. Despite attempts to increase capacity and improve the quality of services, technology companies have fallen short of providing the transparency needed to understand how their practices for moderating content and managing data have frequently failed to provide adequate and timely responses to pressing concerns raised by users in the region, in particular in their own languages.

Efforts to address online harm at the regional and national level have progressed but have been hampered by weak regional human rights standards and institutions.[2] There have only been a few promising examples across the region of states adopting and implementing national action plans for business and human rights.[3] Policy efforts to address the concerns set out in this report will require both strengthening human rights law and policy frameworks as well as the independence of national and regional human rights institutions.

With this global and regional context in mind, the report makes the following six observations about trends that seem to be shaping civic space online in South-East Asia over the last decade:

- **The Spread of Hateful, Misogynistic, and Discriminatory Content.** Hate speech and incitement to violence is spread in an unprecedented fashion with the support of digital tools, particularly affecting marginalized communities and voices promoting public debate such as journalists, HRDs, activists and others, despite efforts to improve the effectiveness of content moderation.

- **Organized and Coordinated Online Attacks and Harassment.** Governments and companies have been complicit in, or failed to take action to stop, online threats and harassment including through trolling, doxing, and the spread of disinformation. Attacks of this kind endanger the safety and security of users and non-users (particularly women, girls, and marginalized individuals).

- **Technologies of Surveillance.** Governments have become sophisticated in the use of digital technologies, including surveillance tools. They have enhanced their capacity to collect and analyse social media and biometric data, established monitoring bodies, and imposed data localization requirements to gain access to private information. Companies have been inconsistent and non-transparent in implementing their policies.

- **Restrictive Legal and Regulatory Frameworks.** Cybercrime, cybersecurity, and other laws regulating digital space have expanded state power to surveil, censor and suppress expression, and invade privacy online. Such laws are often in conflict with international human rights obligations, past commitments to respect human rights and constitutionally guaranteed protections.

- **Criminalization and Prosecution of Online Expression.** Governments are aggressively investigating and prosecuting a wide range of online expression, pursuant to an expanding number of criminal legal provisions. Law enforcement justifies arrests and harsh criminal penalties by reference to public policy aims (such as countering disinformation, hate speech and pandemic measures).

- **Internet Shutdowns and Network Interference.** Internet infrastructure has been threatened by governments seeking to suppress dissent through throttling of bandwidth, blocking of VPNs or other secure communication, DDoS attacks, and other modalities of internet shutdown.

To fulfil the international legal obligations of the United Nations human rights instruments as well as ensure an open, democratic and pluralistic digital space, a deeper understanding of how online hostilities affect civil society and a careful review of the norms and policies adopted to respond to these challenges is vital. A central assertion of this report is that the regulation of digital space – including state regulation and corporate policies – would be most effective if designed in full compliance with international human rights norms and standards.

APPLICABLE INTERNATIONAL LAW AND STANDARDS

Most South-East Asian States have assumed obligations to respect, protect and fulfil human rights by ratifying the International Covenant on Civil and Political Rights (ICCPR) and other treaties (see Annex A). However, even those that are not a party to the ICCPR have an obligation to protect these rights under customary international law and pursuant to other international law commitments. The table below sets out the ratification status of the major international treaties by all of the States in South-East Asia.

The basis of state obligations for protecting rights online is set out in the International Bill of Human Rights, including the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the ICCPR. ICCPR Articles 17 (right to privacy), 18 (freedom of thought, conscience, and religion) and 19 (right to hold opinions without interference, and the right to freedom of expression) are of particular relevance.[4]

The Human Rights Committee that oversees implementation of the ICCPR has elaborated upon these obligations in its General Comments, including establishing that a State is obligated not only to refrain from violating rights, but to protect them from violation by non-state actors, including companies.[5] The Human Rights Committee and other United Nations experts have clarified that these obligations apply to online expression and its regulation.[6] The Optional Protocol of the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography also adds additional obligations to combat child pornography for those States which have ratified.[7] The United Nations has established the Hub for Human Rights and Digital Technology where the reports of these bodies and other key texts pertaining to human rights protections in digital space are compiled.[8]

A central analytical tool for evaluating state interventions that may interfere with digital communications is the test of legality, necessity, proportionality, and legitimacy set out in General Comment 34 of the Human Rights Committee.[9] *Legality* requires that restrictions on expression be imposed pursuant to the law, that it is clearly defined, and that they not allow "unfettered discretion" in their application, or "otherwise contravene international human rights law or standards."[10] *Legitimacy* requires that a restriction fall within the listed objectives set out in ICCPR Article 19 (3) ("ensuring respect of the rights or reputations of others; or… protecting national security, public order or public health or morals"). *Necessity* is only satisfied if no alternative measures existed that would not restrict rights, and *proportionality* requires that restrictions be narrowly-tailored, and the "least intrusive" among available options.[11]

The test applies equally to potential violations of the right to privacy protected under Article 17, as asserted by both the General Assembly and the United Nations High Commissioner for Human Rights.[12] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has described how in the digital realm, the protection of privacy and expression go hand-in-hand, stating that online privacy serves "as a gateway to secure

exercise of freedom of opinion and expression."[13] The Human Rights Committee established that Article 17 (2)'s protection against unlawful interference with privacy extends to unlawful or arbitrary online surveillance, hacking and non-consensual data collection. In addition to having an obligation to refrain from engaging in such activities, States have a positive obligation to protect the right to privacy from infringement by third parties.[14]

Human rights law also prohibits incitement to violence and discrimination and requires governments to take action to curb it. Only when expression reaches the high threshold of incitement does international human rights law require that the State prohibit it. The three-part test under ICCPR's Article 19 remains the primary framework through which to assess the human rights implications of restrictions. Article 20(2) of the ICCPR requires governments to take action to prohibit "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." The Rabat Plan of Action's six-point 'threshold test' helps to operationalize this definition, though its application to large volumes of content presents considerable challenges.[15]

Private sector responsibilities

Although private sector actors do not accrue formal human rights obligations under international customary or treaty law, standards for businesses to protect human rights have evolved dramatically in recent years. In the absence of an international treaty on business and human rights, the primary framework is the United Nations Guiding Principles on Business and Human Rights (UNGPs), unanimously endorsed by the HRC in 2011.[16] The UNGPs re-affirm States' existing duties under international law to protect against human rights abuses by third parties, including business enterprises, and to provide a roadmap to guide States in doing so. They also lay down the corporate responsibility to respect human rights, which requires businesses to avoid infringing upon human rights, and to address adverse human rights impacts in which they may be involved.[17]

The UNGPs' "Respect, Protect and Remedy" framework commits companies to adopt human rights policies, implement due diligence measures, and provide a remedy for harm that they cause or to which they have contributed. UNGPs 17 through 21 set out the basic components of human rights due diligence (assessment, integration of findings, risk mitigation, and external communication).[18] For technology companies, relevant human rights risks include interference with the rights of privacy and freedom of expression and contribution to human rights abuses committed by others (for example, by failing to protect private communications and data or providing a platform for threats or incitement). Under the UNGPs, companies, including network providers, should challenge demands for partial and total shutdowns, take legal action where feasible, and be transparent about government attempts to limit access and their responses to such attempts.[19] The UNGPs also apply to the responsibilities of investors in the technology sector to avoid human rights harm.[20]

TREND 1

HATEFUL AND DISCRIMINATORY SPEECH

© Reuters

Hate speech online and the associated challenges of regulating and moderating social media content is recognized as a critical trend in South-East Asia as it is in the rest of the world. Given the region's ethnic, cultural, and religious diversity, engagement online provides a powerful tool for building solidarity across borders. At the same time, the lack of efficiency of social media content moderation practices combined with a low capacity to detect incidents of incitement is considered to have contributed to discrimination and violence. The documented incidents of online incitement to violence and hatred against Rohingya (see box) are central references for the global debate on the need to improve content moderation.

New forms of online attacks targeting feminist movements and women HRDs (WHRDs), including lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI+) activists, non-binary people and members of sexual minorities can be detected worldwide.[21] United Nations Special Procedures experts have documented the disproportionate impact that online hate speech has had on women journalists, HRDs, activists, and politicians, particularly those from marginalized

communities.[22] A global survey by the United Nations Education, Scientific and Cultural Organization (UNESCO) in 2020 found that 73% of women journalists experienced online gender-based violence.[23] Evidence from South-East Asia reinforces these findings. For instance, there have been measurable increases in various forms of misogynistic online behaviour including trolling and doxing, and spikes in misogynistic posts in several countries.[24] Attacks documented include campaigns against women participating in online discussions[25] to the spread of misinformation, sometimes combined with racist elements.[26]

Government responses to these concerns have often failed to provide adequate protection. As described below, the rapid expansion of frameworks to regulate online space and address concerns with hostilities online has resulted in an increasingly restrictive legal environment that has opened new doors for arbitrary interference, undermining the enjoyment of the rights to privacy and freedom of expression. In some cases, authorities have used legitimate concerns about the impacts of hateful and discriminatory speech against certain groups to justify the undue suppression of certain kinds of online content. Blasphemy laws, for example, are still commonly used to prosecute language viewed as hostile to religion in at least three countries.[27] Newly proposed instruments to address hate speech may further expand the scope for arbitrary interference with freedom of expression.[28]

Social media platforms have failed to anticipate and take action to prevent their products from amplifying hateful and discriminatory speech or addressing harm after the fact. In recent years, platforms have acknowledged that they have not done enough to address the proliferation of hate speech from spreading. For example, although Facebook users are overwhelmingly outside of the United States, only 13% of its 2020 budget for detecting misinformation and other violations of its code of conduct is directed to other countries.[29]

Technology companies have not done enough to prioritize these concerns or direct adequate resources toward addressing them. The lack of an industry standard or a universally accepted definition of hate speech or disinformation in international law also complicates efforts at identifying and responding to these concerns in a consistent and rights-respecting manner, as does the complex linguistic and cultural context of South-East Asia. Expanding definitions of harmful content without adequate sensitivity to the local context can have unintended consequences. This may result in more "false positives," in which material is removed that should not have been, with implications for freedom of expression.[30] Even carefully crafted artificial intelligence solutions to content moderation can result in the perpetuation and reinforcement of discriminatory attitudes and biases.[31]

Finally, while improvements in content moderation are positive steps, more needs to be done to ensure that individuals have effective remedies available to them when they suffer harm, not only as a consequence of content moderation decisions but any actions that infringe on human rights, including to privacy. This should include non-users and communities that are harmed by company action or inaction.[32] International law on the right to an effective remedy should guide regulation by both government and industry.

Incitement Against Rohingya in Myanmar

The Independent International Fact-Finding Mission on Myanmar (IIMM) documented incidents of incitement attacks channelled online targeting the Rohingya in 2017. The IIMM was the first of many international accountability mechanisms to describe the influence of social media, and Facebook in particular, through sharing messages of incitement targeting the Rohingya.[33] Reports from 2018[34] and 2019[35] further addressed the role of social media, namely Facebook, in spreading hate speech. United Nations human rights experts emphasized that the company's response to the spread of hate speech has been slow and ineffective.[36] In 2018, Facebook commissioned a human rights impact assessment of its role in Myanmar. In 2020 the company announced it was working with the IIMM to provide data and relevant information to investigate international crimes in Myanmar.[37]

TREND 2

ORGANIZED ONLINE ATTACKS AND HARASSMENT

© Reuters

Throughout the region, social media and other online platforms have been used to launch organized and coordinated attacks on HRDs and journalists. Large-scale organized online attacks have taken many forms, including organized trolling, doxing, and the coordinated spread of false and defamatory information, organized attacks on websites and applications (for example DDoS attacks), and the use of spyware or malware to target individuals, organizations, or entire communities.

State-sponsored trolling, or persistent and targeted online harassment to intimidate and silence critics, is common in the region and part of a global trend.[38] Trolling takes many forms, including the use of bots or automated messaging software to deliver defamatory messages, disseminate manipulated video or audio content, and spread social media memes alleging misbehaviour or affiliation with criminal organizations. Organized and coordinated efforts utilize tools made available by social media platforms such as micro-targeting of advertising and personalization of news feeds. Sophisticated operations are increasingly skilled at manipulating social media algorithms that promote contentious and polarizing content that amplify the effect of trolling.

Powerful economic actors and dominant political groups, sometimes aligned with past or present governments, have used third parties to troll critics or disseminate threatening memes about critics or opponents, making it difficult to establish a clear link to State actors. And while these third parties may include so-called "troll farms" and other clandestine operations, attacks also occur in the open via social media influencers, ideologically or politically aligned online communities and popular figures with a large online audience. In some cases, governments support non-state actors to engage in a mix of online and offline attacks against critics.

The Special Rapporteur on the situation of HRDs has drawn attention to the linkages between online and offline threats, noting that killings of HRDs can be "presaged by online and offline threats, including death threats."[39] These threats are often gendered and include threats of rape and other gender-based violence.[40]

The organized harassment frequently coincides in a context where State or non-state actors are also actively promoting disinformation. Coordinated campaigns spreading disinformation online and through other mainstream media and official channels can encourage attacks against critics or those who hold unpopular views. In some cases, they are narrowly targeted at undermining the credibility and authority of particular civil society actors or journalists.

"Doxing," or the disclosing of other people's personal information without consent, is a particularly nefarious form of harassment because the sharing of personal information can be interpreted as an implicit invitation for others to take action offline – including physical violence. It frequently has a gendered nature and impact, such as the sharing of sexual or other intimate images without consent, often with a view towards silencing, delegitimizing and deterring women and girls from participating in public spaces. While various forms of trolling, doxing, and spreading of defamatory and false information are illegal in many jurisdictions, enforcing these restrictions can be a challenge, even for well-intentioned governments with limited technical capacity. The fact that there is no agreed upon legal and technical definition of these terms further complicates its regulation. Concerns have been voiced by OHCHR and United Nations human rights mechanisms about the alleged direct and indirect support of State actors and intelligence units for collecting and disclosing personal information.[41]

The response of social media companies to state-sponsored or sanctioned trolling, harassment and disinformation has been slow but improving. From a human rights perspective, the approach adopted by social media platforms has a number of weaknesses. There are no industry-wide shared definitions for organized and coordinated attacks or common standards governing how such attacks should be addressed. Although transparency about decision-making has improved somewhat, it remains opaque and subject to inadequate oversight. Companies have also focused enforcement in affluent, Western countries while these issues remain largely unaddressed in the rest of the world (where most users live).

Meta has progressively developed policies on what it called "coordinated inauthentic behaviour," defining it as campaigns that include groups of fake accounts and pages seeking to mislead people about who they are. In a recent overview of the enforcement of its policy against this

practice between 2017 and 2022, Meta informed that it has acted against over 200 operations globally, noting that around 90% of the influence operations identified in the Asia-Pacific region were wholly or partly focused on domestic audiences (including cases of Government agencies targeting their own population).[42]

Trolling and "red tagging" in the Philippines

The High Commissioner for Human Rights noted the threat that red-tagging poses to civil society in a report on the situation of human rights in the Philippines while indicating that some of these defamatory campaigns are channelled through social media, directly affecting HRDs, journalists and politicians.[43] In January 2021, multiple United Nations Special Rapporteurs sent a communication outlining similar concerns about online smears and "red tagging" of human rights activists, including allegations of surveillance of the victims by the military, death threats from paramilitary groups, and coordinated online attacks.[44] The Philippines responded to the Special Procedures communication.[45]

TREND 3

ABUSE OF DIGITAL SURVEILLANCE TECHNOLOGIES

© Reuters

Online technologies also significantly expand the opportunities for monitoring individuals and organizations as underlined repeatedly by the High Commissioner.[46] The global market of surveillance tools has thrived over the last decade and South-East Asian governments are part of this trend, purchasing new tools and investing in the expansion of their technical capacity. This includes the purchase of hardware and software to monitor social media activity, as well as more invasive forms of surveillance, such as the collection and use of facial recognition and biometric data. The proliferation of these technologies has been enabled by a poorly regulated export regime for surveillance technology to which even the most authoritarian governments can avail without regard for their human rights impact.[47]

Surveillance technologies have been exported to South-East Asia clandestinely or with minimal transparency. Countries in the region have installed security cameras and implemented facial recognition technology in urban areas with foreign assistance.[48] A recent study has pointed out that some cities in South-East Asian have the highest number of security cameras per square mile in the world.[49]

Private companies from outside the region have also played a role in supplying hacking and surveillance software to governments that have subsequently been used to target journalists and HRDs.[50] Researchers have noted that its surveillance and hacking technology were detected in devices used by journalists and HRDs working in at least two South-East Asian countries.[51] NSO's Pegasus phone hacking software was also detected on the devices of activists and protesters in at least two countries in the region.[52] Activists in the region were also targeted by the spyware "Candiru."[53] Cellebrite, which manufactures hacking and surveillance software, has entered into partnerships with South-East Asian governments.[54]

While analysing overall trends in the market and use of new surveillance technologies, including multiple revelations regarding the use of malware targeting HRDs and journalists, the High Commissioner has called on States to "implement moratoriums on the domestic and transnational sale and use of surveillance systems, such as hacking tools and biometric systems that can be used for the identification or classification of individuals in public places, until adequate safeguards to protect human rights are in place."[55] United Nations human rights experts made similar calls.[56]

There has been a proliferation of (often militarized) bodies to oversee the deployment of these technologies, ostensibly to fight against cybercrime and other illegal activity online. Some are embedded in law enforcement agencies, and others are separate but forward cases to police and prosecutors for investigation. Other bodies are integrated into intelligence agencies and/or controlled by the military.

The existing legal and institutional frameworks fail to establish independent controls and oversight mechanisms, which are needed for these bodies to operate in a transparent and accountable manner or with effective judicial oversight. Procedural standards for the implementation of surveillance provide significant discretion for executive authorities, increasing risks of arbitrary interferences with privacy. Policy responses to COVID-19 have exposed another problematic dimension of state surveillance as governments developed tools to track the spread of the pandemic. Digital contact tracing applications that collect personal data, including biometrics, were introduced quickly and without public discussion or oversight. As in other parts of the world, at least seven countries in South-East Asia reportedly implemented some form of digital contact tracing, all characterized by a lack of transparency, unclear policies, and considerable security vulnerabilities.[57] The negative impacts of such surveillance in response to COVID-19, as well as its use for the delivery of public health benefits and services, are potentially far-reaching.[58]

Most countries in the region lack a law protecting personal data or have a law with broad exemptions for information collected by the government.[59] Reports raised concerns about the sharing between government officials of biometric or mobile tracking data obtained by security agencies during the pandemic.[60] For example, United Nations experts expressed concern about the lack of safeguards (or legislative framework) to prevent data collected through proposed tracking tools from being accessed by multiple authorities and used for purposes unrelated to the management of the pandemic.[61]

Also in line with global trends, some South-East Asian authorities are collecting and analysing the content of communications stored and shared through social media and other networks built on publicly accessible communications. The monitoring of online communication in the region is further enabled by regulations that require companies and network providers to maintain user data within the territory of the country so that the authorities can exercise legal (including criminal) jurisdiction over the production and dissemination of communications and data. Requests for access to data collected by telecommunications and internet service providers have increased globally, often supported by newly adopted mandatory data retention laws.[62] In South-East Asia, a growing number of countries (at least five at present) impose some type of data localization requirement.[63]

Companies in the region are also insufficiently transparent about their responses to government requests for communications data and content. Legal instruments sometimes limit the ability of companies to share information about the requests they receive. Some social media platforms have started to provide data about government requests through transparency reports. However, the quality of information shared with individuals affected by requests and the public in general is still minimal. This includes social media platforms that cooperate with or help enable government surveillance as well as companies providing hardware and software to governments for ostensibly legitimate purposes, such as aiding law enforcement or contact tracing, when they know or have good reason to believe that they will be misused.[64]

Cambodia – Responses to the COVID-19 crisis

In March 2022, the United Nations Human Rights Committee expressed deep concern "about the persistent violation of the freedom of expression (…)" and alarm at the reported "closure of multiple national and international media outlets; the blockage of websites critical of the Government; the use of criminal and civil legal actions against journalists and human rights defenders; and the widespread harassment and intimidation of online activists, including during the elections in 2018, and for criticizing the State party's handling of the COVID-19 pandemic." The Committee noted with concern "that some criminal offences contained in the Criminal Code and in the Law on Telecommunications[65], including defamation, incitement, insult and lese-majesty, are often used to restrict freedom of expression disproportionately and excessively" and also noted concern over the Sub-Decree on the National Internet Gateway[66] and new draft legislation, including on cybercrime and access to information, and the draft amendments to the Press Law" which raised, according to the Committee, serious concerns regarding further limitations on freedom of expression.[67]

In a communication sent in March 2021, two United Nations Special Rapporteurs expressed concern about potential risks posed to the right to privacy by the introduction of a QR Code system named "Stop Covid." They noted with concern the lack of specific measures to protect the privacy and data of individuals and the lack of assurances that the data collected would be accessible and used only by those directly involved in the pandemic response management.[68] Cambodia responded to the Special Procedures communication.[69]

Cybersecurity in Viet Nam

In 2019, and again in 2022,[70] the United Nations Human Rights Committee expressed concerns about the "severe restriction on freedom of expression," namely as a result of Articles 109, 116, 117 and 331 of the Penal Code of Viet Nam. The Committee also indicated concern about the Law on the Press of 2016, which establishes State control over the media, and the Law on Cybersecurity of 2018 which prohibits the use of internet services, to criticize the State. Lastly, they highlighted the "arbitrary arrest, detention, unfair trials and criminal convictions" of HRDs, journalists, bloggers and lawyers for criticizing State authority.[71] The Committee recommended an urgent review of the legislation. In 2021, three United Nations Special Rapporteurs called on the Government to halt the application of Articles 117 and 331 of the Penal Code in a communication outlining their concerns about the arbitrary detention and legal prosecution of HRDs and candidates for the 2021 elections for the National Assembly.[72] Viet Nam responded to the Special Procedures communications.[73]

TREND 4

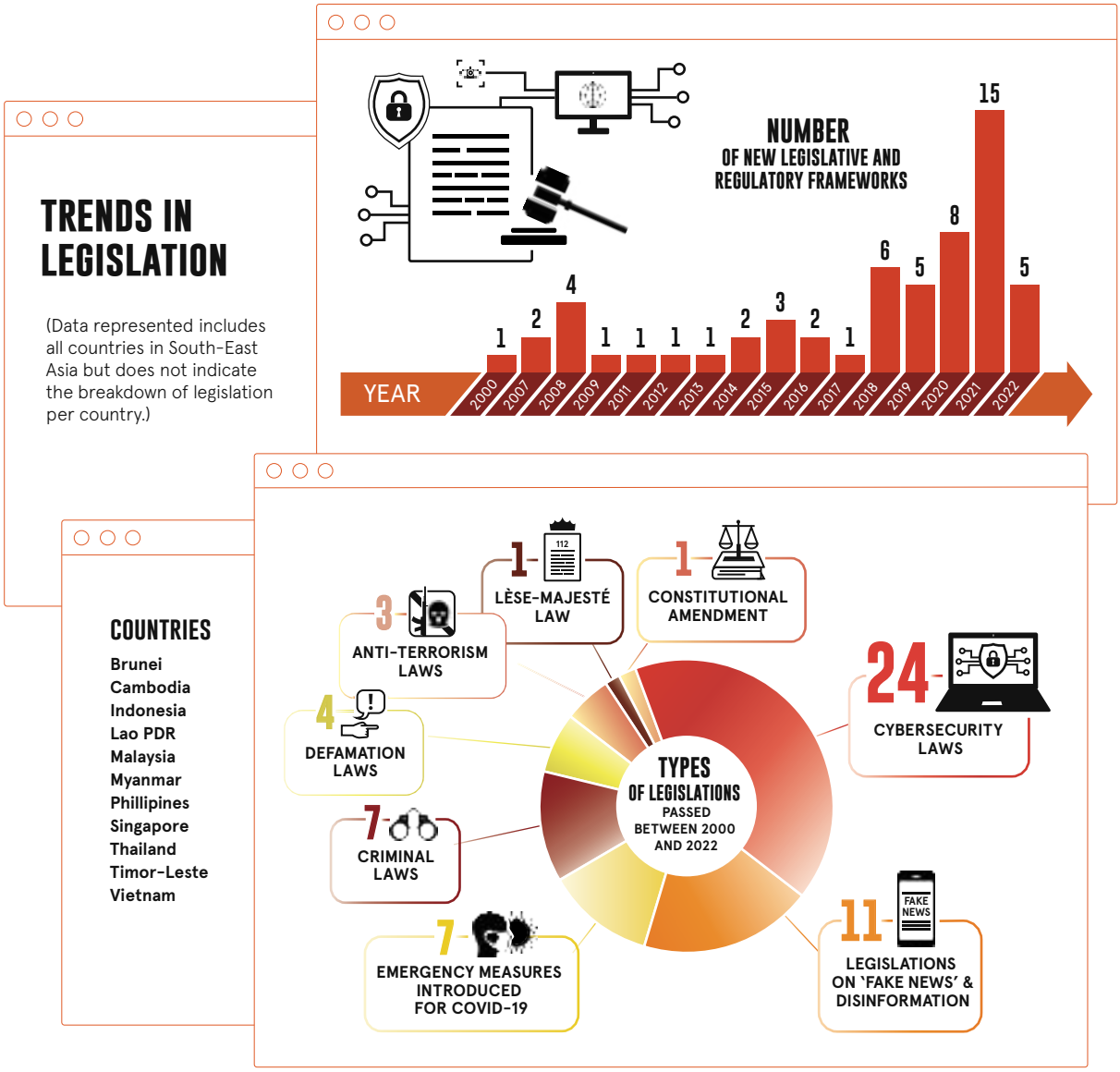
RESTRICTIVE LEGAL AND REGULATORY FRAMEWORKS

© Sirinarth Mekvorawuth | Dreamstime.com

Laws or regulations that infringe upon or constrain online expression are enforced in all countries in the region. Governments target online expression by relying upon existing legal frameworks historically used to suppress dissent, including overbroad laws governing national security and counter-terrorism, states of emergency, criminal defamation (including lèse-majesté), NGO registration and even tax laws. Weak formulations of the constitutional and legal right to freedom of expression further increase the risks of excessive restrictions.

In recent years, however, an array of new laws has been introduced with the aim of addressing online space that further expand the scope of these provisions to explicitly encompass expression on social media and in other digital spaces.[74] These more recent laws take several forms, including regulatory frameworks meant to: (a) prevent the dissemination of false information (so-called "fake news" laws); (b) securing computer systems from attack and failure ("cybersecurity" laws); and (c) incorporate online space into the broader regulatory

framework (various telecommunications and computer crime laws). Although these laws may have legitimate policy objectives on the surface, they have often expanded state power and restricted speech without offering well-reasoned and proportionate policy solutions.



While all laws need to be analysed with their specific context in mind, human rights provide guardrails for what is permissible. From that perspective, many of the laws share a set of recurrent problematic provisions. Some laws have borrowed language from legislation in other countries without embedding the new norms in the pre-existing legal landscape and assessing their implications for fundamental freedoms. This regulatory trend is not limited to South-East Asia as other regions have also adopted similar laws aiming at tackling concerns with issues such as cyber-crime, child protection online, or hate speech and disinformation presenting similar flaws.[75]

A non-comprehensive list of human rights concerns associated with these laws include:

- **Vague and overbroad definitions.** Many laws leave important terminology undefined or provide poorly articulated definitions that make them prone to misinterpretation or deliberate misapplication (for instance, terms such as 'public order', 'national security', 'peace and tranquillity', 'fake news', and 'misleading or false information').

- **Expansive discretion for officials.** Many of these laws create broad scope for arbitrary and political interferences empowering law enforcement personnel or officials at various levels of government to make determinations about violations and the severity of their punishment without adequate independent supervision or recourse to appeal decisions to a judicial body.

- **Compelling access to user data.** New laws frequently impose penalties on social media companies or network providers that refuse to take measures to make it easier for authorities to access user information, such as keeping user data within the country (data localization), reducing encryption, blocking VPNs, providing "backdoor" access to systems, or acquiescing to over broad government requests for user data.

- **Disproportionate criminal penalties.** Laws often criminalize lawful expression (such as defamation) and impose unnecessary and disproportionate penalties – extending in some cases to life imprisonment and crippling fines that result in the destruction of livelihoods.

- **Extra-Territorial application.** Increasingly, legislation seeks to extend criminal jurisdiction to include content regardless of where it originates. This creates legal vulnerabilities for non-citizens or critics-in-exile and incentivizes over-enforcement by platforms seeking to avoid legal liability in multiple jurisdictions.

- **Lack of judicial oversight.** Many laws do not require an application to the judiciary to compel the handover of user data or other information, bypass existing judicial safeguards, or place legal and administrative obstacles in the way of those seeking an independent review of decisions such as the removal of content.

- **Intermediary liability.** Laws are increasingly including provisions that make social media companies and network providers liable for third-party content posted on their platforms. Some laws go a step further and extend criminal liability to certain corporate staff located in the country, subjecting them to potential arrest and prosecution if a platform disseminates or fails to remove allegedly illegal content.

In addition to laws governing digital spaces and technologies, reportedly, at least 110 countries worldwide made pandemic-related emergency declarations with implications for freedom of expression and association, including over 278 COVID-19-related legal measures enacted in South-East Asia – often bypassing regular consultations and democratic legislative processes.[76] While recognizing the need to tackle concerns such as disinformation in the context of the pandemic, United Nations human rights mechanisms and experts repeatedly warned about

the human rights impacts of such government overreach.[77] These legal frameworks provided the legal basis for government requests to social media platforms to remove content critical of the authorities, block social media accounts and sites that are technically in violation of local law, or otherwise limit access. Combined with additional instruments, including criminal law provisions, they constitute tools that allow the violations documented elsewhere in this report to occur.

The influence of new laws that aim to address concerns relating to the spread of hate speech and disinformation online is transnational. The new generation of "fake news" laws and their COVID-19-related enhancements, are borrowing from one another.[78] Germany's Network Enforcement Act, NetzDG, adopted in 2017 with the aim of ensuring platforms' content moderation remove hate speech violating German law is considered to have influenced legislation in over 26 countries in all regions, including in South-East Asia.[79]

By following basic human rights and rule of law principles, governments can avoid enacting laws and policies that do not meet international standards and result in human rights violations and curtailment of freedoms. The recommendations in this report build upon past guidance that OHCHR has issued to lawmakers on how to ensure that laws and regulations governing digital space are consistent with human rights law.[80]

Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA)

The United Nations Special Rapporteur on Freedom Expression expressed concerns about the law's compatibility with international human rights standards in a communication[81] sent to authorities in April 2019. He expressed concern that the then-bill would, if adopted, give authorities virtually unfettered discretion to label and restrict expressions they disagree with as "false statements of fact." The communication further indicated that the Bill could "lead to the criminalization and suppression of a wide range of expressive conduct, including criticism of the government, and the expression of unpopular, controversial or minority opinions" and disproportionately affect HRDs and journalists. Singapore replied to the Special Procedures communication.[82]

Malaysia's Emergency (Essential Powers) (No. 2) Ordinance 2021

The United Nations Special Rapporteur on Freedom of Expression sent a communication in March 2021[83] outlining her concerns about the Ordinance's provisions and enquired about incompatibility with international human rights law, similar to the repealed Anti-Fake News Act of 2018. Concerns included the overly broad definition of "fake news" in the Ordinance, which could criminalize legitimate expressions and allow criminal punishment without requiring that those disseminating the "fake" information knew that it was false or intended to publish fake information. The communication also indicated concern on the heavy penalties stipulated in the Ordinance, which appeared to be inconsistent with the requirements of necessity and proportionality. The Emergency Ordinance was revoked on 8 December 2021. Malaysia did not respond to the communication sent by the Special Rapporteur.[84]

TREND 5

ARRESTS AND PROSECUTIONS IN RELATION TO EXPRESSION ONLINE

© Reuters

Arrests and prosecutions for online expression, including social media posts, are becoming increasingly frequent in the South-East Asia region. While there is no readily available data to accurately estimate the number of criminal actions brought against HRDs, journalists, and other critics for online activity, the problem is widespread and part of a global trend.

Defamation laws that authorize third parties, not just prosecutors, to bring criminal actions have also created a surge of so-called 'cyber-libel' cases against HRDs and journalists brought by corporations, politicians, and government officials. The United Nations Special Rapporteur on the situation of HRDs observed that such cases are part of a broader pattern of abuse by government officials and companies that undermines accountability and good governance and diminishes civil society's role in holding them accountable, "lead[ing] to the silencing of important voices in a society."[85]

According to a recent analysis, in 2021, 75% of people globally "live in countries where people were arrested or imprisoned for posting content online," where reliable data is available.[86] The study identified reports of arrests or convictions for social media posts in nine countries in the South-East Asia region.[87]

Concerns about the spread of alleged misinformation and disinformation relating to the COVID-19 pandemic have also been used as a justification to expand restrictions and to criminalize a broad range of speech critical of state responses to the pandemic in the region. The prosecution of HRDs and journalists for online criticism is part of a larger crackdown on civic space. In June 2020, the High Commissioner issued a statement highlighting the misuse of pandemic-related emergency decrees by several South-East Asian governments to justify the arrest of critics of pandemic policy for social media posts, online publications, and works of art.[88] This use of COVID-19 measures to prosecute critics for expression unrelated to the pandemic is part of a well-documented global trend.[89]

Numerous cases involving the criminal prosecution for online content have been brought to the attention of United Nations Special Procedures mandate holders, including regarding arrests and prosecutions of HRDs for statements they made on issues such as police and military abuse, corruption, and discrimination. The United Nations Special Rapporteur on the situation of HRDs noted that the increase in allegations may indicate that government officials and companies are using their broad powers to issue subpoenas on HRDs and then refer HRDs to law enforcement using the information gathered via subpoena. The prosecution of individuals often relies on data extracted from platforms directly by State actors or obtained from platforms through legal proceedings. To respond to these concerns, some social media platforms have designed additional tools to support the protection of HRDs in high-risk environments, such as enhancing security protections for and control over accounts or conducting human rights impact assessments that consider the specific vulnerabilities of HRDs.

Thailand: Defamation and lèse-majesté

The Human Rights Committee expressed its deep concern at the sharp increase in the number of persons detained and prosecuted for the crime of lèse-majesté since the military coup in Thailand in 2014. It stressed, in its concluding observations in 2017, that the State Party should revise Article 112 of its Penal Code on public insult to the royal family to bring it in line with Article 19 of the ICCPR.[90] In accordance with its General Comment No. 34, the Committee further reiterates that the detention of persons for exercising their right to freedom of expression violates Article 19 of the ICCPR.[91]

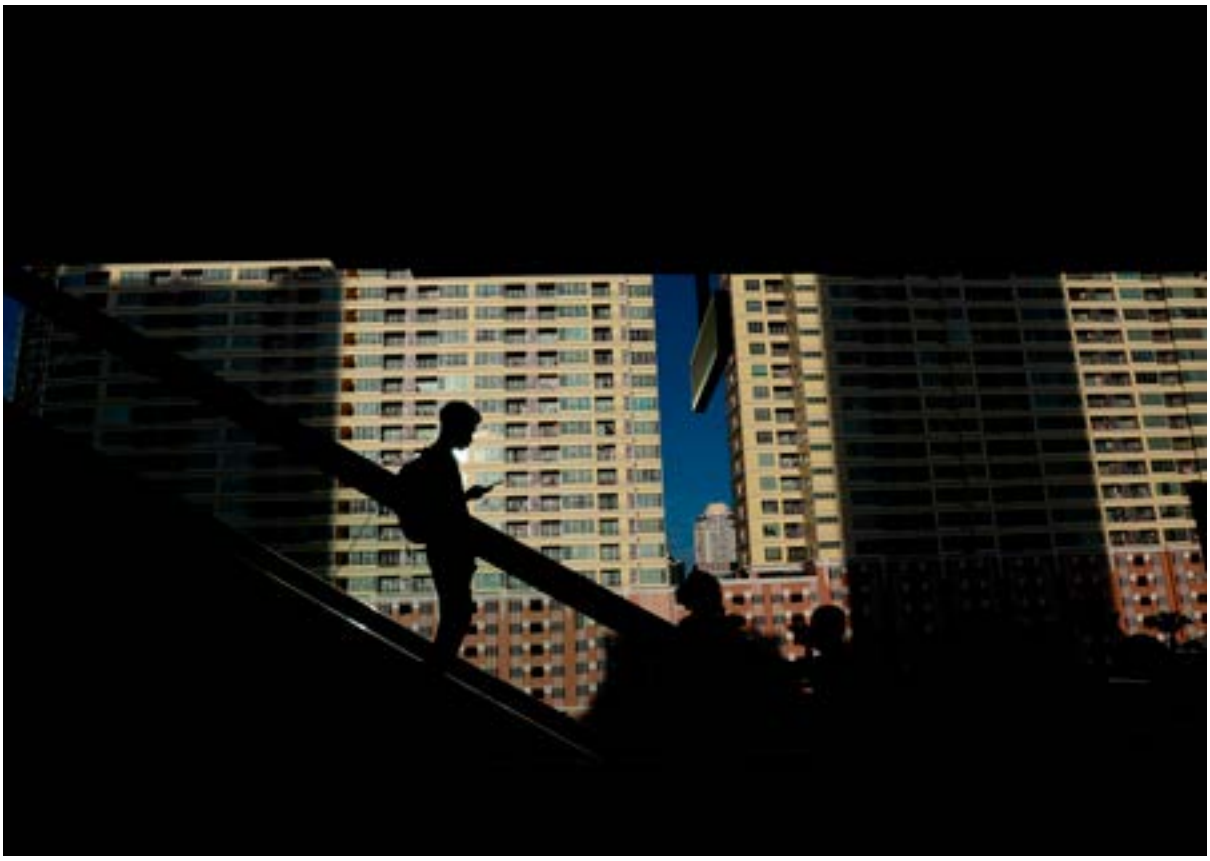
Similar concerns were also reflected by several United Nations Special Rapporteurs about the application of lèse-majesté laws in Thailand. In 2011, the UN special rapporteur on freedom of expression urged the government to amend its defamation and lèse-majesté laws to conform with the country's international human rights obligations.[92] Concern was expressed in public statements in 2017[93], 2020[94], and 2021[95], on allegations of various cases of lèse-majesté prosecutions and, in some cases, arrests of civil society actors making references to their communications online.[96]

Lao PDR – Criminalization of expression

United Nations Special Rapporteurs sent a communication in 2016[97] and 2021[98] detailing their concerns about the arrests of HRDs in connection with posts on Facebook criticizing the Government of Lao PDR[99] and emphasized their concern about the vaguely defined offences of defamation, libel and insult, and the criminalization of the online criticism of the Government or of circulating false or misleading information online, and called on the State to revise these laws with a view to guaranteeing the full enjoyment of freedom of expression.

TREND 6

INTERNET SHUTDOWNS AND NETWORK INTERFERENCE



© Reuters

Partial or total internet shutdowns appear at the extreme end of government tactics and responses with severe direct and indirect implications for the enjoyment of all human rights.[100] Internet shutdowns are commonly understood as measures taken by a government, or on behalf of a government, to intentionally disrupt access to information and communications systems and prevent their use. Shutdowns may include complete blocks of internet connectivity or accessibility of the affected services or simply throttling bandwidth while maintaining only low quality online access. Another form of mandated disruption is to limit the availability of some websites and services, including social media. In some cases, shutdowns include blocking telephone networks.

The use of internet shutdowns as a tool is extremely hard to justify under international human rights law, if it is possible at all. Given their indiscriminate and disproportionate reach and impact, they fail the tests of necessity and proportionality set out by the Human Rights Committee in General Comment No. 34.[101] They are by nature an unnecessary and disproportionate

response, even when legitimate concerns exist. The devastating impacts of shutdowns on the economy, public health, freedom of expression and other rights (including the rights to work, health, and education), have been extensively documented including by the High Commissioner for Human Rights.

The #KeepItOn Coalition recorded 31 shutdowns in the region between 2016 and 2021.[102] South-East Asian governments utilize a range of tools to block or limit access to the internet, although complete disruptions are relatively rare.

As the impact of shutdowns becomes clearer, in other regions, courts have stepped in to question the legal or constitutional basis for shutdowns – sometimes after public protests or civil society advocacy. This suggests the potential for some level of judicial oversight in even the most sensitive political cases as well as the potential power of advocacy to reverse shutdown decisions.[103]

The consequences of shutdowns during a pandemic are particularly severe in terms of access to health information.[104] The Human Rights Council consequently called on States "to refrain from… the use of Internet shutdowns to intentionally and arbitrarily prevent or disrupt access to or the dissemination of information online" and on business enterprises "to meet their responsibilities under the UNGPs."[105] These responsibilities include being transparent about, and where possible, challenging (including in court) government demands to shut down internet access.[106]

Internet shutdowns and network interference in Myanmar

A number of United Nations human rights mechanisms expressed concerns about the impact of internet shutdowns over the last few years. For example, in 2019[107] and 2021[108] concerns were publicly expressed. Most recently, in June 2022, United Nations Special Rapporteurs condemned the "digital dictatorship" and called on the international community to protect the fundamental rights to freedom of expression, access to information and privacy of the people of Myanmar.[109] The report of the High Commissioner for Human Rights to the Human Rights Council in May 2022, noted that "The World Bank recently calculated that Internet shutdowns in Myanmar alone had cost nearly $2.8 billion between February and December 2021, reversing economic progress made over the previous decade."[110]

Indonesia – Internet disruption in the Papua region

In September 2019, the High Commissioner for Human Rights and five United Nations human rights experts publicly expressed concerns in separate statements[111] on the escalating violence in the Papua region and the reported disruption of internet services. The group of experts emphasized that "access to the internet contributes to preventing disinformation and ensuring transparency and accountability."[112] The High Commissioner also noted that "blanket internet shutdowns are likely to contravene freedom of expression and limiting communications may exacerbate tensions."[113]

CONCLUSION AND RECOMMENDATIONS

The six trends identified in this report reflect a global communications environment that is being rapidly reshaped by new technological developments and regulations. Understanding and responding adequately to the risks posed by the spread of incitement, the increase in organized attacks and the expansion of surveillance are challenges for all. Developing and implementing norms and policies that ensure that online space is safe and inclusive is complex, given the transnational nature of digital domains and the limited understanding of how online communications function today.

Concerns related to cybercrime, terrorism or hate speech and incitement online result in the adoption of laws and policies all over the world, often without due diligence in conducting impact assessments and diverse and meaningful consultations. The desire to respond swiftly to complex challenges generates new norms and policies that, rather than promoting safety online, risk providing space for arbitrary State interventions, deepening authoritarian practices, and restricting civic space and fundamental freedoms.

This report draws attention to the many recent laws and regulations regarding the online space in South-East Asia, many of which appear to reinforce and expand pre-existing restrictions of freedoms of expression, association and privacy. They have significant and often adverse implications for journalists, HRDs, bloggers, environmental and social activists and civil society organizations. These effects range from the disruption of their work, financial duress, personal threats and attacks, arrest and detention, judicial harassment and criminalization, enforced disappearances and forced closure of civil society organizations.

The report describes how online space mirrors offline tensions. Technological innovation opens up space for advocacy on the one hand and, on the other, increases avenues for restrictions. The global market of surveillance tools is expanding unabated, supplying governments in all contexts with tools to hack and monitor individuals and systematically surveil online, public space and discourse with minimal safeguards for internet users. Social media platforms can also be manipulated with the support of bots and used as channels for coordinated campaigns vilifying or threatening civil society actors. In addition, companies' lack of adequate resource allocation and attention provided to certain communities and their limited capacity to moderate content and provide support in non-European languages deprives multiple users of timely responses to incitement cases or protection demands.

A holistic approach, fully anchored in human rights, is needed to effectively reverse the trends identified in this report. Such an approach is vital if the international community, private companies, and national governments are to successfully mitigate the harm caused by ongoing violations, secure accountability for past abuses, and establish human rights-protective and gender-responsive laws and policies in the future.

Given the novelty and technical complexity of some of these issues, more research, including comparative research, is needed in South-East Asia and beyond. Effective policy solutions require a new level of transparency, cooperation, and commitment to human rights principles by governments, companies, investors, civil society, and intergovernmental institutions.

RECOMMENDATIONS

A. ANCHOR LAWS AND POLICIES IN HUMAN RIGHTS, IN PARTICULAR FREEDOM OF EXPRESSION AND PRIVACY

International human rights law provides a recognized transnational set of rules on freedom of expression and the right to privacy, elaborated by experts from around the globe. It should underlie any regulation of digital space and technology. Assessing the impact of laws that affect public freedoms and privacy online on an ongoing basis is critical to ensuring that they meet the tests of legality, legitimacy, proportionality and necessity. Similarly, it is urgent to understand the effects of the proliferation of the sale and use of surveillance technologies and respond accordingly.

Recommendations to States:

- Repeal any law that criminalizes or unduly restricts expression, online or offline. Laws and policies regulating online spaces (and the processes for developing and implementing them) must be consistent with international human rights law.[114] Pursuing a legitimate objective is not sufficient for justifying restrictions on freedom of expression. Instead, they must be necessary and proportionate to achieve the legitimate purpose, they must not be overbroad, and the State has an obligation to demonstrate in a specific and individualized fashion links between the threat and the necessity and proportionality of the measures imposed.[115]

- Adopt strong, robust and comprehensive privacy legislation, including on data protection, that complies with international human rights law. Adequate oversight of State surveillance practices requires the urgent establishment of fully independent and adequately resourced mechanisms.

- Refrain from blocking access to the internet through partial or total internet shutdowns and network throttling.

- End the sale, export, import and use of privately developed and owned surveillance hardware and software until human rights-respecting regulatory frameworks are in place.

Recommendations to companies:

- Ensure that their internal policies, including platform codes of conduct, are aligned with human rights and the UNGPs. Corporate policies should make specific reference to human rights instruments and adopt definitions of key terms.

B. ENSURE DUE PROCESS, TRANSPARENCY AND ACCOUNTABILITY

Given the serious impact of interventions by States and companies in online expression and privacy, it is imperative that those affected are informed and have recourse to appeal or can seek a remedy for decisions that impact or harm them. A fully independent and adequately resourced justice system is a precondition for fairly and effectively implementing the normative framework.

Recommendations to States:

- Ensure that any State measures to restrict or interfere with online content are based on an order by an independent and impartial judicial authority, in accordance with due process and standards of legality, necessity and legitimacy, and are implemented transparently.

- Ensure that State surveillance conducted for public health purposes, such as pandemic control measures, is limited, conducted transparently and in accordance with the law, subject to oversight (including by an independent judiciary) and protects personal data and other privacy requirements.

- Ensure accountability for cases of incitement to hatred and violence.

- Invest in broader measures to counter hate speech, such as promoting counter speech, fomenting public participation and debate, and human rights education.

- Promote access to information, media freedom and information/digital literacy, empowering individuals to identify and critically analyse and counter disinformation.

- Seek to ensure that government officials condemn and refrain from disseminating hate speech or disinformation. Government officials or entities must also refrain from sponsoring covert or public coordinated online campaigns aimed at directly attacking and disqualifying civil society and media actors.

Recommendations to companies:

- Provide effective remedy in accordance with Principle 22 of the UNGPs, where they have caused or contributed to a rights violation. A human rights approach to a remedy requires consideration of all of its aspects: satisfaction, restitution, non-repetition, rehabilitation and compensation. Non-judicial mechanisms should align with the effectiveness criteria of Guiding Principle 31.[116]

- Telecommunications companies and network providers should exhaust all domestic remedies to challenge shutdown requests and implement shutdown requests narrowly, with the goal of keeping communications channels as open as possible, and take all lawful measures to enable the full and immediate disclosure of information about all orders to disrupt communications.

- Social media companies should review content moderation policies and processes to ensure they align with international human rights standards. Platforms must expand transparency at all stages of their operations, systematically providing data on the implementation of their content moderation policies and process, including all interferences implemented at the request of governments. Platforms must also provide accessible channels for challenging their moderation decisions.

- Companies involved in the development, dissemination, and application of surveillance technologies must integrate human rights due diligence processes from the earliest stages of product development, marketing and use, taking all appropriate action to ensure that their products are not used to violate human rights.

C. UPHOLD THE PRINCIPLE OF INCLUSIVITY AND PARTICIPATION

Too often, civil society has been left out of the process of developing laws and policies that affect civic space online – sometimes in deliberate attempts to evade public scrutiny and accountability. Governments and companies must listen to and act upon civil society concerns and ensure broad consultation in law and policymaking processes. Policy solutions must ensure that digital space is safe and accessible regardless of gender, socio-economic status, religious and ethnic identity, and other factors.

Recommendations to States:

- Institute gender-responsive laws and implement them so that they protect journalists and HRDs from legal harassment and online intimidation.

- Take all steps necessary to address the digital divide through the implementation of gender-responsive policies that specifically seek to overcome barriers to access and ensure equal and affordable internet access to all people and communities regardless of gender, race, religion, political affiliation, or economic status.

Recommendations to companies:

- Commit to transparent, inclusive, gender-responsive engagement with civil society in all its diversity, not only about human rights impacts but also product design and implementation, to ensure technologies are equally accessible and do not perpetuate discrimination or undermine democratic processes.

- Expand collaboration with local civil society and media entities promoting the protection of HRDs and journalists and commission reviews of the impact of online attacks and intimidation against these groups, including gendered harassment and discriminatory behaviour. In coordination with local actors, consider adopting policy, product, and operational changes in order to advance the protection of journalists and HRDs.

- Social media companies must invest more in services in the different languages used in the region and significantly expand the capacity of human review of content moderation processes in the languages in use with consideration of contextual issues.

D. STRENGTHEN REGIONAL AND NATIONAL HUMAN RIGHTS INSTITUTIONS

The ASEAN Intergovernmental Commission on Human Rights (AICHR) and National Human Rights Institutions can contribute to preserving the space for debates about the impact of digital technologies and responses to them in the region. These entities should play an active role in documenting and investigating online violations and facilitating the exchange of experience in relation to regulatory and policy responses.

Recommendations to the ASEAN:

- ASEAN States should properly resource National Human Rights Institutions, refrain from influencing or interfering in such a way as to compromise their independence and provide them with legal or constitutional mandates that allow them to engage independently and proactively on all human rights issues, including those pertaining to business and human rights.

- AICHR should interpret its mandate broadly and advocate with ASEAN States for the expansion of its protection mandate. In the meantime, it should exercise its powers to initiate dialogue with technology companies, strengthen engagement with a diversity of civil society and deploy the tools at its disposal (such as thematic studies) to address digital rights issues.

Recommendations to National Human Rights Institutions

- Actively monitor and investigate attempts to restrict online freedom and to abuse online tools to intimidate or silence civil society actors; contribute with impact assessments of the use of new technology; and actively engage with civil society, policymakers, companies and international human rights mechanisms in order to inject human rights in all efforts to promote access to the internet as well as online safety and inclusion.

ENDNOTES

1 United Nations Guidance Note: Protection and Promotion of Civic Space, September 2020, at https://www.ohchr.org/Documents/Issues/CivicSpace/UN_Guidance_Note.pdf

2 "UN experts raise concerns over 'landmark' Southeast Asian human rights declaration," UN News, 16 November 2012, at https://news.un.org/en/story/2012/11/425852; "UN official welcomes ASEAN commitment to human rights, but concerned over declaration wording," *UN News*, 19 November 2012, at https://news.un.org/en/story/2012/11/426012; for civil society legal analysis, see International Commission of Jurists, *The ASEAN Human Rights Declaration: Questions and Answers*, 30 July 2013, at ; Forum-Asia, *A Decade in Review: Assessing the Performance of the AICHR to Uphold the Protection Mandates*, 24 June 2019, at https://www.forum-asia.org/?p=29041

3 For updated information on the status of national action plans, see Office of the High Commissioner for Human Rights, "National action plans on business and human rights," at https://www.ohchr.org/EN/Issues/Business/Pages/NationalActionPlans.aspx

4 For additional information about the UN treaty bodies, please see https://www.ohchr.org/en/treaty-bodies

5 UN Human Rights Committee, General Comment No. 34, CCPR/C/GC, 12 September 2011, para. 7, at https://undocs.org/CCPR/C/GC/34; see also, Committee on the Rights of the Child, General Comment No. 25 (2021) on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021, at https://undocs.org/CRC/C/GC/25

6 United Nations Human Rights Council, *The promotion, protection, and enjoyment of human rights on the Internet*, 4 July 2018, A/HRC/38/L.10/Rev.1, at https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/7

7 Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, art. 3, para. 1(c). The UN Committee on the Rights of the Child has noted in this context, however, that "(A)ny restrictions on children's right to freedom of expression in the digital environment, such as filters, including safety measures, should be lawful, necessary and proportionate", see, General Comment No. 25 (2021) on children's rights in relation to the digital environment, paras 59, 69 and 70.

8 United Nations Human Rights and Digital Technology Resource Hub, at https://www.digitalhub.ohchr.org/

9 "Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the socio-political system espoused by the government."

10 General Comment No. 34, CCPR/C/GC, paras. 25-26.

11 Ibid, paras. 33-35.

12 UN General Assembly resolutions A/RES/71/199 and A/RES/75/176, https://undocs.org/en/A/RES/71/199; Human Rights Council resolutions AHRC/51/17 and A/HRC/RES/48/4; Report of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31, 13 September 2021, para. 8, at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

13 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, 28 May 2019, A/HRC/41/35, para. 24, at https://undocs.org/A/HRC/41/35

14 Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, para. 27 28 May 2019 at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement; UN Human Rights Committee, General Comment No. 31, CCPR/C/21/Rev.1/Add.13, 26 May 2004, at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G04/419/56/PDF/G0441956.pdf?OpenElement

15 Office of the High Commissioner for Human Rights, *Freedom of expression vs incitement to hatred: OHCHR and the Rabat Plan of Action*, at https://www.ohchr.org/EN/Issues/FreedomOpinion/Articles19-20/Pages/Index.aspx

16 Office of the High Commissioner for Human Rights, United Nations Guiding Principles on Business and Human Rights: "Implementing the United Nations "Protect, Respect and Remedy" Framework (2011), at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

17 For a detailed analysis of these responsibilities in the context of new technologies, see the High Commissioner for Human Rights B-Tech Project at https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.

18 Principles 17 through 21, *United Nations Guiding Principles on Business and Human Rights*, at https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

19 Office of the High Commissioner for Human Rights, *Internet Shutdowns and Human Rights*, at https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

20 UN Human Rights B-Tech Project, *Rights Respecting Investment in Technology Companies*, at https://www.ohchr.org/Documents/Issues/Business/B-Tech/B-Tech-Briefing-Investment.pdf

21 Report of the Special Rapporteur on violence against women, A/HRC/38/47, 18 June 2018, at https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/OnlineViolence.aspx

22 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the UN General Assembly, 30 July 2021, A/76/258, at https://undocs.org/A/76/258; Report of the Special Rapporteur on violence against women, *Combating violence against women journalists*, A/HRC/44/52, 6 May 2020, paras. 39-52, at https://undocs.org/A/HRC/44/52; Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/75/184, 20 July 2020, at https://undocs.org/A/75/184; Report of the Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity, A/76/152, 15 July 2021, at https://undocs.org/a/76/152

23 UNESCO, Online violence against women journalists: a global snapshot of incidence and Impacts (2020), at https://unesdoc.unesco.org/ark:/48223/pf0000375136

24 UN Women, *Social Media Monitoring on COVID-19 and Misogyny in Asia and the Pacific*, August 2020, at https://mythoslabs.org/2020/08/06/researching-the-impact-of-covid-19-on-online-misogyny-in-asia/; UN Women, *Standing Up to the Challenge: Response to the COVID-19 Pandemic in Asia and the Pacific*, December 2020, p. 8, at https://asiapacific.unwomen.org/en/news-and-events/events/2021/02/report-launch—standing-up-to-the-challenge

25 Harsono, Andreas, "Brave Indonesian Women Discuss Freedom to Choose What to Wear," Human Rights Watch, 25 February 2021, at https://www.hrw.org/news/2021/02/25/brave-indonesian-women-discuss-freedom-choose-what-wear; Facebook also acknowledged cyberbullying and harassment against outspoken women on the platform in its response to its own human rights impact assessment and adapted online harassment policies to address the concern. Facebook, *Response to Indonesia Human Rights Impact Assessment*, at https://about.fb.com/wp-content/uploads/2021/03/FB-Response-Indonesia-HRIA.pdf and Meta, Advancing Our Policies on Online Bullying and Harassment, at https://about.fb.com/news/2021/10/advancing-online-bullying-harassment-policies/

26 Sastramidjaja, Yatun and Amirul Adli Rosli, "Tracking the Swelling COVID-19 Vaccine Chatter on TikTok in Indonesia," *ISEAS Yusof Ishak Institute* 17, June 2021, at https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2020-82-tracking-the-swelling-covid-19-vaccine-chatter-on-tiktok-in-indonesia-by-yatun-sastramidjaja-and-amirul-adli-rosli/; Gavin Butler, "How Sinovac Became the Poster Child of Anti-Chine, Anti-Vaxx Skepticism, *Vice*, 3 August 2021, at https://www.vice.com/en/article/qj8xgd/sinovac-anti-china-covid-vaccine-skepticism

27 Harsono, Andreas, "Indonesia to Expand Abusive Blasphemy Law," *Human Rights Watch*, 31 August 2019, at https://www.hrw.org/news/2019/10/31/indonesia-expand-abusive-blasphemy-law; Human Rights Watch, "Brunei: New Penal Code Imposes Maiming, Stoning," 3 April 2019, at https://www.hrw.org/news/2019/04/03/brunei-new-penal-code-imposes-maiming-stoning; Article 19, *Briefing Paper: Blasphemy Provisions in Malaysian Law*, January 2021, at https://www.article19.org/wp-content/uploads/2021/01/2021.01.20-Malaysia-blasphemy-briefing-paper-final.pdf

28 See, Article 19, "Myanmar: Government's approach to 'hate speech' fatally flawed," 4 May 2020, at https://www.article19.org/resources/myanmar-governments-approach-to-hate-speech-fundamentally-flawed/; Article 19, "Malaysia: Efforts to combat 'hate speech' should not trample freedom of expression," 27 August 2019, at https://www.article19.org/resources/malaysia-efforts-to-combat-hate-speech-should-not-trample-freedom-of-expression/

29 Murphy, Hannah, et al., "Four revelations from the Facebook Papers," *ars technical*, 26 October 2021, at https://arstechnica.com/tech-policy/2021/10/four-revelations-from-the-facebook-papers/ Meta reports having spent USD$5 billion on safety and security in 2021 alone, and indicating it had 15,000 people who review content in more than 70 languages, in over 20 locations.

30 Evelyn Douek, "COVID-19 and Social Media Content Moderation," *Lawfare,* 25 March 2021, at https://www.lawfareblog.com/covid-19-and-social-media-content-moderation; Evelyn Douek, "More Content Moderation Is Not Always Better," Wired, 2 June 2021, at https://www.wired.com/story/more-content-moderation-not-always-better/

31 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29 August 2018, paras. 36-38, at https://undocs.org/A/73/348

32 Jenny Domino, "How Myanmar's Incitement Landscape Can Inform Platform Regulation in Situations of Mass Atrocity," *Opinio Juris*, 2 February 2020, at https://opiniojuris.org/2020/01/02/how-myanmars-incitement-landscape-can-inform-platform-regulation-in-situations-of-mass-atrocity/

33 Report of the Independent International Fact-Finding Mission on Myanmar, 27 August 2018, at paras. 34, 74, at https://www.ohchr.org/EN/HRBodies/HRC/MyanmarFFM/Pages/ReportoftheMyanmarFFM.aspx

34 A/HRC/39/64 at para. 73, 74, at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/274/54/PDF/G1827454.pdf?OpenElement

35 A/HRC/42/50 at para. 72, 75, at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/236/74/PDF/G1923674.pdf?OpenElement

36 A/HRC/39/CRP.2 at para 2352, at https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_CRP.2.docx,

37 Meta, "An Independent Assessment of the Human Rights Impact on Facebook in Myanmar," at https://about.fb.com/news/2018/11/myanmar-hria/

38 Monaco, Nicholas, et al, Institute for the Future, *State-sponsored Trolling: How Government Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns* (2018), at https://www.iftf.org/statesponsoredtrolling/

39 Special Rapporteur on the situation of HRDs, *Final warning: death threats and killings of human rights defenders*, A/HRC/46/35, 24 December 2020, paras. 50, 62, at https://undocs.org/en/A/HRC/46/35

40 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the United Nations General Assembly, 30 July 2021, A/76/258, paras. 62-67, at https://undocs.org/A/76/258

41 See for instance, OHCHR's reports: A/HRC/51/17, paras 4-7, 18; A/HRC/35/9, paras 19, as well as reports by the UN Special Rapporteur on the right to freedom of expression: A/HRC/50/29, paras 36-37, 44-46; UN Special Rapporteur on violence against women, A/HRC/38/47, paras 42, 47, 57; A/HRC/44/52, paras 33, 42; and the UN Special Rapporteur on the right to privacy, A/77/196, paras A/HRC/41/35.

42 Meta, Recapping Our 2022 Coordinated Inauthentic Behavior Enforcement, 15 December 2022 at https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/

43 Human Rights Council, Report of the United Nations High Commissioner for Human Rights to the General Assembly, 29 June 2020, A/HRC/44/22 at para. 49–62, at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/156/66/PDF/G2015666.pdf?OpenElement

44 Mandates of the Working Group on Arbitrary Detention; the Special Rapporteur on extrajudicial, summary or arbitrary executions; the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on the rights of indigenous peoples and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 11 January, 2021, AL PHL 1/2021, at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25942

45 Response by the Philippines dated 1 February 2021 to the Special Procedures allegation letter is available at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=35937

46 Human Rights Council, The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/51/17 and other privacy reports

47 Ibid.

48 Ross Andersen, "The Panopticon is Already Here," *The Atlantic*, September 2020, at https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

49 Bischoff, Paul, "The World's Most-Surveilled Cities", 11 July 2022, at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

50 Krapiva, Natalia and Hinako Sugiyama, Access Now, "Why spy firm Cellebrite can't hide from investors," 26 May 2021, at https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/; Joint civil society letter, "Cellebrite should not go public without demonstrating human rights compliance," 13 July 2021, at https://www.accessnow.org/cms/assets/uploads/2021/07/CSO_Open-Letter_on_Cellebrite.pdf; Oded Yaron, "What Viet Nam is Doing With Israeli Phone-hacking Tech," *Haaretz, 15* July 2021, at https://www.haaretz.com/israel-news/tech-news/.premium-what-vietnam-is-doing-with-israel-s-phone-hacking-tech-1.10003831; Mclaughlin, Timothy , "Security tech companies once flocked to Myanmar: One firm's tools were used against two journalists,"

Washington Post, 4 May 2019, at https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html; Page, Carly, "Apple alerts NSO phone hacking victims in Thailand, El Salvador and Uganda," *TechCrunch*, 25 November 2021, at https://techcrunch.com/2021/11/24/apple-nso-hacking-notify/

51 Joint civil society letter, "Cellebrite should not go public without demonstrating human rights compliance," 13 July 2021, https://www.accessnow.org/cms/assets/uploads/2021/07/CSO_Open-Letter_on_Cellebrite.pdf; Oded Yaron, "What Viet Nam is Doing With Israeli Phone-hacking Tech," *Haaretz,* 15 July 2021, at https://www.haaretz.com/israel-news/tech-news/.premium-what-vietnam-is-doing-with-israel-s-phone-hacking-tech-1.10003831

52 Scott-Railton, John, et al, The Citizen Lab, "GeckoSpy Pegasus Spyware Used against Thailand's Pro-Democracy Movement", 17 July 2022 at https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/ and Carly Page, "Apple alerts NSO phone hacking victims in Thailand, El Salvador and Uganda," *TechCrunch*, 25 November 2021, at https://techcrunch.com/2021/11/24/apple-nso-hacking-notify/

53 Marczak Bill, et al, The Citizen Lab, " Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus, 15 July 2021 at https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/

54 The company did break some of these ties in the run-up to an initial public offering. See Access Now, "Why spy firm Cellebrite can't hide from investors," 24 May 2021, at https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/

55 A/HRC/51/17, 56 (g).

56 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Surveillance and human rights*, 28 May 2019, A/HRC/41/35, para. 2, at https://undocs.org/A/HRC/41/35; see also, Statement by the United Nations High Commissioner for Human Rights, Committee of Legal Affairs and Human Rights, Council of Europe, Hearing on the implications of Pegasus Software, 14 September 2021, at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E

57 Digital Reach, *The Pandemic of Surveillance: Digital Contract Tracing in Southeast Asia*, at https://digitalreach.asia/digital-contact-tracing-regional/

58 Mandate of the Special Rapporteur on extreme poverty and human rights, Report to the UN General Assembly, A/74/493, 11 October 2019, at https://undocs.org/A/74/493

59 Singapore, Malaysia, and the Philippines have laws in place. However, the Singapore and Malaysia laws have exemptions for government. *Digital Reach Regional Overview*, at 3.

60 In Thailand, a civil society submission to UPR raised concerns about the sharing between government officials of biometric or mobile tracking data obtained by security agencies during the pandemic. Joint UPR Submission Thailand, at 4.7. Digital Reach, The Pandemic of Surveillance: Philippines, at https://digitalreach.asia/digital-contact-tracing-philippines; see also, Foundation for Media Alternatives, A Pandemic as Vector for State Surveillance and Other Abuses, September 2021, at https://fma.ph/2021/09/13/a-pandemic-as-vector-for-state-surveillance-and-other-abuses/ According to the Philippines in its reply on 31 January 2023, sent in response to a NV by OHCHR, stating the following:"the NPC conducted a compliance check in 2020 and provided comments on the app's Privacy Impact Assessment (PIA). Numerous meetings and consultations were likewise held among the NPC, Multisys, the Department of Health (DOH), Department
of Information and Communications Technology (DICT), and other government agencies before the said app was turned over by Multisys to the Philippine government, specifically to the Department of the Interior and Local Government (DILG) in 2021."

61 Mandates of the Special Rapporteur on the situation of human rights in Cambodia; the Special Rapporteur on the right of everyone to the enjoyment of the highest obtainable standard of physical and mental health, *Communication concerning the development of a QR Code system named "Stop Covid" to prevent the spread of COVID-19*, AL KHM 1/2021, 18 March 2021, at https://cambodia.ohchr.org/sites/default/files/othersource/Joint%20Letter%20by%20UN%20experts%20on%20QR%20Code%20System%20to%20Stop%20COVID-19.pdf. The government's response can be found at https://cambodia.ohchr.org/sites/default/files/othersource/Response%20from%20the%20Government%20to%20the%20UN%20experts%20on%20the%20QR%20Code%20System%20to%20stop%20COVID-19.pdf

62 Human Rights Council, The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3 August 2018, at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement

63 Shahbaz, Adrian, et al, *Freedom House, User Privacy or Cyber Sovereignty: Assessing the Human Rights Implications of Data Localization* (July 2020), at https://freedomhouse.org/sites/default/files/2020-07/FINAL_Data_Localization_human_rights_07232020.pdf

64 Report of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/48/31, 13 September 2021, paras. 55-56, at https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high

65 On 13 January 2023, the PM of Cambodia noted, in response to a NV by OHCHR, the following: "the Law on Telecommunications which was promulgated in late 2015 is to ensure the effective, safe, quality, reliable, affordable telecommunication infrastructure, to protect telecommunication users and to increase national budget. This law was formulated with the consultation from Japan International Cooperation Agency (JICA), International Telecommunication Union (ITU), Inter-ministries and compared with best practices and laws from other countries including, Thailand, Singapore, Malaysia, Japan, and the Republic of Korea. This article aims to protect privacy and safety of telecommunications users as mentioned in the article 65 (the basic rights of telecommunication users) of the law. However, this law is to be updated and amended to be in line with international standards and the fast development of technology."

66 On 13 January 2023, the PM of Cambodia noted, in response to a NV by OHCHR, in relation to the Sub-Decree on National Internet Gateway (NIC), the following: "this Sub-Decree does not restrict or suppress the freedom of expression or collect user data and conversations. NIG laws have been established in almost all countries and Cambodia is no exception. NIG will be run by private operators and installed in various sites across the country and along the borders, operated in accordance with international standards. The Sub-Decree was prepared in a transparent manner, and consultations were held with experts in the telecommunication sector, private operators, and relevant institutions on numerous occasions. The purpose of NIG is to increase the effectiveness of national revenue collection on the basis of fair and honest competition, and transparency between the state and operators, as well as to prevent illicit activities such as illegal cross-border network connections, illegal online gambling, cyber threats, pornography, and online frauds and scams. In addition, NIG will facilitate, strengthen, and manage internet connection domestically and internationally, thereby enhancing internet service quality. The Sub-Decree and the establishment of such NIG adhere to the principles of legality, necessity and proportionality, and contribute to the realization of Cambodia's vibrant digitalization, a driving force to growth and development. Again, this vital tool was passed for a legitimate goal – to facilitate and manage internet connections, to strengthen national security and tax collection, and to help maintain social order and protect national culture. The establishment of NIG does not violate people's freedom of expression, but instead contributes to the protection of communities in the cyberspace and a healthier online environment. Under the Sub-Decree, private operators shall cooperate with the Royal Government and take measures only in various circumstances such as protection of national security and public order and morals, which is in line with internationals norms and especially the International Covenant on Civil and Political Rights. The attainment of the Kingdom's digitalization and development relies upon regulating and restraining businesses from engaging in unethical and unlawful practices."

67 The Human Rights Committee's concluding observations on the third periodic report of Cambodia dated March 2022, at https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fKHM%2fCO%2f3&Lang=en, para 34. On 13 January 2023, the PM of Cambodia noted, in response to a NV by OHCHR, the following: "the Inter-Ministerial Prakas No. 170 on the management of publication on website and social media processing via internet in the Kingdom of Cambodia is intended to clarify the roles and responsibilities in addition to the existing laws. It aims to mention the clear division of responsibilities between competent government institutions: the Ministry of Interior, Ministry of Information and the Ministry of Post and Telecommunications."

68 AL KHM 1/2021, at https://cambodia.ohchr.org/sites/default/files/othersource/Joint%20Letter%20by%20UN%20experts%20on%20QR%20Code%20System%20to%20Stop%20COVID-19.pdf Cambodia responded to the Special Procedure communication on 7 May 2021, at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=36202

69 On 13 January 2023, the PM of Cambodia noted, in response to a NV by OHCHR, the following: "The Cambodian Ministry of Post and Telecommunications (MPTC) and Ministry of Health initiated a QR Code Technology System "Stop COVID-19" that aims to assist with contact tracing of new Covid-19 cases. This system was to combat the spread of the covid-19. to assist individuals exposed to Covid-19 to self-quarantine, get tested and treated timely to prevent spread of the virus. In this digital era, the Stop-Covid app is an essential system that helps protect the public health, public safety, and ensure economic wellbeing of the country, and the rights and freedom of others. Stop-Covid was introduced not only in Cambodia, but also used in other countries where there was an outbreak of covid-19. The Scanned QR Code technology system records only mobile phone of the users who voluntarily use the QR Code. No other private data is recorded.

The individual's right to privacy enshrined in the Constitution of Cambodia and related laws and international instruments including the ratified international human rights treaties, the Civil Code, the Criminal Code, and the Law on Telecommunications. In this regard, MPTC would like to clarify the purpose of the QR code technology as follows:

1. Accessibility to the collected data from this public health measure is restricted to only a specific list of people belonging to the top management of the Committee and granted only when the location of an outbreak is identified. 2. The data will be automatically deleted after 28 to 90 days depending on the significance of the information. 3. The data is securely stored and encrypted by MPTC. Different security levels are also applied in accordance with international standards. 4. The contact tracing by using QR Code "Stop Covid-19" is for the specific purpose of public health measure and it is not compulsory. 5. In case individuals wish to raise their concerns about violations of their rights to privacy, they can report to the Committee, MPTC or Telecommunication Regulator of Cambodia."

70 CCPR/C/136/2/Add.4, Report on follow-up to the concluding observations of the Human Rights Committee https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fVNM%2fFCO%2f3&Lang=en

71 Human Rights Committee, Concluding observations on the third periodic report of Viet Nam, CCPR/C/VNM/CO/3 at para. 45(a)–(d), at docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhslrjZYHLHPYdqrup6FR%2FpxpoKD6CFGnGSaZiMZA5cstApQ4%2FLSGVGL6rHlXBfZYdGh1DO9LG7%2BM6pkcuSoJ7H38G4X1D4w%2B0PGGRuCuB0OlW

72 Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the situation of human rights defenders AL VNM 4/2021, 1 November 2021, at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26688

73 Viet Nam's response to the Special Procedures can be found at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=36703 (21 December 2021) and https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=37431 (24 March 2023)

74 For a review of these laws as of December 2019, see International Commission of Jurist, *Dictating the Internet: Curtailing Free Expression, Opinion and Information Online in Southeast Asia*, 11 December 2019, at https://www.icj.org/southeast-asia-icj-launches-report-on-increasing-restrictions-on-online-speech/

75 For an analysis of the impacts of the German law, see Tworek Heidi and Paddy Leerssen, "An Analysis of Germany's NetzDG Law," *Transatlantic Working Group*, 15 April 2019, at https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

76 International Center for Not for Profit Law, "Government Responses to COVID-19 in Asia and the Pacific," accessed on 12 November 2021, at https://www.icnl.org/post/analysis/government-responses-to-covid-19-in-asia-and-the-pacific

77 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Disease pandemics and the freedom of opinion and expression*, 23 April 2020, A/HRC/44/49, para. 24, at https://undocs.org/A/HRC/44/49

78 Han Kirsten, "How Singapore's 'fake news' law gets exported," The Ballot, 8 April 2021, at https://www.theballot.world/articles/singaporefakenews

79 The Report of the Select Committee of the Singapore Parliament, as well as a green paper from the Ministry of Communication and Information and Ministry of Law, made specific reference to NetzDG. See Parliament of Singapore, "Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures," at https://www.parliament.gov.sg/sconlinefalsehoods and Jacob Mchangama and Natalie Alkiviadou, https://justitia-int.org/wp-content/uploads/2020/09/Analyse_Cross-fertilizing-Online-Censorship-The-Global-Impact-of-Germanys-Network-Enforcement-Act-Part-two_Final-1.pdf

80 Moderating online content: fighting harm or silencing dissent?", *Office of the High Commissioner for Human Rights*, 23 July 2021, at https://www.ohchr.org/EN/NewsEvents/Pages/Online-content-regulation.aspx

81 Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL SGP 3/2019, at https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Legislation/OL_SGP_3_2019.pdf

82 The Permanent Mission of the Republic of Singapore, in its response to the Special Rapporteur on 5 July 2019, notes "several errors" and a "central misconception" in the SR's understanding regarding certain provisions of the Bill, including concerns raised regarding the scope of judicial oversight of the Bill, timeline and related issues and concerns linked to the process of bringing statutory appeals to court noting that these will be prescribed in the Bill's subsidiary legislation. The Government also notes that the definition of a "false statement of fact" in the Bill in Clause 2(1), noted by the SR as problematic, reflects existing national jurisprudence in areas as criminal, tort, and contract law, which can be used by the court in its statutory interpretation of the Bill, after it becomes law, in compliance with Section 9A(3) c of the Interpretation Act. The Government has also rejected concerns raised by the SR that the Bill authorises Ministers to adjudicate the criminality of statements "effectively reversing" the presumption of innocence highlighting that administrative directions regarding the Bill do not bring criminal liability on any person, do not make statements illegal and simply require a correction to be made, or, in some serious cases, a falsehood to be taken down.
The full response can be accessed at https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=34769

83 OL MYS 5/2021, 25 March 2021, at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26287

84 On 30 January 2023, the PM of Malaysia noted, in response to a NV by OHCHR, the following: "the Malaysian Emergency (Essential Powers) (No.2) Ordinance 2021 is no longer in implementation. The Government noted the Ordinance was time-bound and its enforcement was merely an immediate response to the pandemic. Suffice to say that Malaysia executed a pandemic response that was people-centred, proportionate, necessary and non-discriminatory."

85 "Indonesia: Stop judicial harassment of HRDs - UN expert," 26 November 2021, at https://www.ohchr.org/en/press-releases/2021/11/indonesia-stop-judicial-harassment-human-rights-defenders-un-expert

86 Shahbaz Adrian and Allie Funk, *Freedom House, Freedom on the Net 2021: The Global Drive to Control Big Tech*, pp. 6-8, at https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech

87 Between June 2020 and May 2021. Ibid, p. 7.

88 OHCHR, "Asia: Bachelet alarmed by clampdown on freedom of expression during COVID-19," 3 June 2020, at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25920&LangID=E

89 Civil society space: COVID-19: the road to recovery and the essential role of civil society - A/HRC/51/13, p.24-26, at https://www.ohchr.org/en/documents/thematic-reports/ahrc5113-civil-society-space-covid-19-road-recovery-and-essential-role

90 Concluding observations on the second periodic report of Thailand, CCPR/C/THA/CO/2, para 38, at https://www.ohchr.org/en/documents/concluding-observations/ccprcthaco2-concluding-observations-second-periodic-report

91 Human Rights Committee's General Comment No. 34 (CCPR /C/GC/34) para 9, at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

92 Thailand / Freedom of expression: UN expert recommends amendment of lèse majesté laws, 10 October 2011, at https://www.ohchr.org/en/press-releases/2011/10/thailand-freedom-expression-un-expert-recommends-amendment-lese-majeste-laws

93 Thailand: UN rights expert concerned by the continued use of lèse majesté laws prosecutions 6 February 2017, at https://www.ohchr.org/en/press-releases/2017/02/thailand-un-rights-expert-concerned-continued-use-lese-majeste-prosecutions

94 Press briefing notes on Thailand, at https://www.ohchr.org/en/press-briefing-notes/2020/12/press-briefing-notes-thailand

95 Thailand: UN excerpt alarmed by rise in use of lese-majeste laws, 8 February 2021 at https://www.ohchr.org/en/press-releases/2021/02/thailand-un-experts-alarmed-rise-use-lese-majeste-laws

96 On 19 January 2023, the PM of Thailand noted, in response to a NV by OHCHR, the following: "the rights to freedom of expression and freedom of assembly are guaranteed under the Thai Constitution" and reaffirmed Thailand's commitment to "uphold[ing] the obligations under the ICCPR", including on the rights to fair trial. The PM indicated the representatives from relevant agencies often met with protest leaders to hear their concerns" and "peaceful demonstrations have been facilitated by the authorities. In some demonstrations, especially the ones without clear leaders, tension and frustration may have led to confrontations and aggravation of violence. Thailand further noted that the exercise of these rights must be within the boundary of the law and not infringe upon the rights and reputation of others or instigate hatred and undermine national security and public order. Thailand also stated that "officers may not arrest any person without a warrant or a court order unless there is an urgent need to do so" and "the suspect in a criminal case shall be presumed innocent". In relation to the section 112 of Thailand's Criminal Code, the PM indicates that there is an increase in the use of lèse-majesté Law and that "the purpose of the lese-majeste law, enshrined in Section 112 of the Thai Criminal Code, is not solely to protect the Monarch, Queen or Heir (…) the Section also protects the institution of the monarchy which is revered by the majority of the Thai people. Therefore, the law serves to uphold public order and national security, which warrants appropriately severe penalties, once thoroughly considered."

97 Mandates of the Working Group on Enforced or Involuntary Disappearances; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the independence of judges and lawyers, UA LAO 3/2016, 25 July 2016, at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=3281

98 Mandates of the Special Rapporteur on the situation of human rights defenders; the Working Group on Arbitrary Detention; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the rights of freedom of peaceful assembly and of association, UA LAO 2/2021, at https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=26318

99 Human Rights Committee, Concluding observations on the initial report of the Lao People's Democratic Republic CCPR/C/LAO/CO/1 at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/347/38/PDF/G1834738.pdf?OpenElement

100 Human Rights Council, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, 13 May 2022, A/HRC/50/55, at https://undocs.org/Home/Mobile?FinalSymbol=a%2Fhrc%2F50%2F55&Language=E&DeviceType=Desktop&LangRequested=False

101 Ibid.

102 The #KeepItOn coalition is comprised of over 244 civil society organizations that have systematically recorded episodes of Internet shutdowns in a public database after corroboration. The count of reported shutdowns incidents correspond to the aggregation of data displayed in the coalition's public database for the years between 2016 and 2021. See www.accessnow.org/keepiton/#coalition. https://docs.google.com/spreadsheets/d/1DvPAuHNLp5BXGb0nnZDGNoiIwEeu2ogdXElDvT4Hyfk/edit#gid=1098610033

103 Such victories by civil society are far too rare, but have also been seen in India, Pakistan, Sudan, Togo and Zimbabwe. Internet Society, "Policy Brief: Internet Shutdowns," 18 December 2019, at https://www.internetsociety.org/policybriefs/internet-shutdowns/

104 Human Rights Council, Disease pandemics and the freedom of opinion and expression, 23 April 2020, A/HRC/44/49, paras. 24-29, at https://undocs.org/A/HRC/44/49

105 United Nations Human Rights Council, Freedom of Opinion and Expression, 24 July 2020, A/HRC/RES/44/12, at https://undocs.org/en/A/HRC/RES/44/12

106 Office of the High Commissioner for Human Rights, *Internet Shutdowns and Human Rights*, at https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human

107 "Government internet ban leaves parts of Myanmar 'in a blackout', UN expert calls for immediate lifting", 24 June, 2019, at https://news.un.org/en/story/2019/06/1041161

108 "Internet shutdowns now 'entrenched' in certain regions, rights council hears", 1 July 2021, at https://news.un.org/en/story/2021/07/1095142

109 Myanmar: UN experts condemn military's "digital dictatorship", 7 June 2022, at https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship

110 A/HRC/50/55 at para. 34.

111 UN High Commissioner for Human Rights' comment on Indonesia (Papua and West Papua), 04 September 2019, at https://www.ohchr.org/en/press-releases/2019/09/comment-un-high-commissioner-human-rights-michelle-bachelet-indonesia-papua

112 "Indonesia must protect rights of Veronica Koman and other reporting on Papua and West Papua protests – UN experts," OHCHR (16 September 2019), at https://www.ohchr.org/en/press-releases/2019/09/indonesia-must-protect-rights-veronica-koman-and-others-reporting-papua-and

113 On 31 January 2023, the PM of the Republic of Indonesia noted, in response to a NV by OHCHR, the following: the internet restriction in Papua in August-September 2019 "was carried out to swiftly re- establish security in the area after the protest and riot as an effect of the incident in Surabaya. This step was temporary and implemented because of the wide circulation of false information, hoaxes, and discriminative statement through the internet." Access to internet was fully recovered approximately two weeks after the restriction was initiated. The comment also noted that on 3 June 2020, the Jakarta State Administrative Court, in response to claims filed by several parties against the internet shutdown, ruled that "the action of the Government had breached the law" and that "the Government has accepted the verdict as a self-correction mechanism for policies that have been issued". The comment also noted that the Government provided written responses to communications received from UN experts through two joint communications No. AL IDN 7/2019 and AL IDN 8 /2019.

114 For a more detailed breakdown of these principles, see OHCHR , "Regulating Online Content – the Way Forward," at https://www.ohchr.org/Documents/Press/Regulating-online-content-the-way-forward.pdf

115 Human Rights Committee, General Comment 34, CCPR/C/GC/34 paras. 33 and 35.

116 UN Human Rights B-Tech Project, *Designing and implementing effective company-based grievance mechanisms*, at https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-company-based-grievance-mechanisms.pdf; *Access to remedy and the technology sector: basic concepts and principles*, at https://www.ohchr.org/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf