ONLINE CONTENT REGULATION IN THE ASIA-PACIFIC

Limiting Civil Society's Capacity to Hold Governments Accountable

ASIACENTRE

ONLINE CONTENT REGULATIONS IN THE ASIA-PACIFIC

Limiting Civil Society's Capacity to Hold Governments Accountable

2024

Asia Centre

Asia Centre
65/168, Chamnan Phenjati Business Center Building 20th Floor, Rama 9 Road,
Huai Kwang, Huai Kwang,
Bangkok, 10310 , Thailand
contact@asiacentre.org

ABBREVIATIONS

ASEAN	Association of Southeast Asian Nations
CCA	Computer Crime Act (2007) (Thailand)
CSO	Civil Society Organisation
DSA	Digital Security Act (2018) (Bangladesh)
IMDA	Infocomm Media Development Authority (Singapore)
INGO	International Non-governmental Organisation
ISP	Internet Service Provider
NIG	National Internet Gateway
PECA	Prevention of Electronic Crimes Act (2016) (Pakistan)
POFMA	Protection from Online Falsehoods and Manipulation Act (2019) (Singapore)
UGC	User-generated Content
UU ITE	Information and Electronic Transactions Law (2008) (Indonesia)

CONTENTS

Page

Abbreviations IV
Executive Summary V

1. Introduction 1
1a. Methodology 1
1b. Definition of Key Terms 1
1c. The Digital Communications Landscape 2
1d. Changed Patterns of Information Consumption 5
1e. Digital Tools for Advocacy 6

2. Online Content Regulations in the Asia-Pacific 8
2a. Penal Codes and National Security Laws 8
2b. Electronic and Computer Usage Law 10
2c. Fake News Law 11
2d. Laws on Service and Digital Platforms Providers 12
2e. Internet Infrastructure Laws 13

3. Impact on Internet Freedoms 15
3a. Criminalising Criticism of Government Policies 15
Individual Activists and Leaders 15
Independent Media Houses and CSOs 17
3b. Requesting Legal Compliance from ISPs and Technology Companies 18
3c. Internet Shutdowns and Internet Gateways 20
3d. Trolling, Cybertroopers, Hate Sites 21
Trolling and Cybertroopers 22
Hate Sites 23
3e. Rise of Self-Inhibiting Behaviours Among INGOs and CSOs 24

4. Recommendations 26

5. Conclusion 28

Bibliography 29

EXECUTIVE SUMMARY

The existing and emerging suite of online content regulation in the Asia-Pacific have limited civil society's capacity to hold governments accountable. Individuals and organisations that engage in online advocacy are increasingly persecuted and prosecuted, resulting in a range of self-inhibiting behaviours. This has overall weakened their effectiveness in calling for accountability of government policies. This weakness has to be addressed.

Since the early 2000s, the internet has become widely popular across South Asia, Southeast Asia, and East Asia – although remarkable differences exist between the internet penetration indices of these regions. Access to the internet enabled the widespread use of social media platforms and messaging applications, which have become indispensable tools of communications for millions of people.

The rapid expansion of digital technology and communication has opened up a myriad of opportunities for active political involvement. These opportunities range from the democratisation of information access – providing instant entry to an almost endless array of sources representing diverse views and publishers from various backgrounds – to the prospect of interacting with political leaders through websites, social media platforms, and messaging applications.

However, numerous challenges have surfaced with the emergence of new possibilities for political empowerment. Governments have updated penal codes and national security laws, enacted fake news and cybersecurity laws as well as laws that govern internet service providers and technology companies. These laws have widely been used to block and remove online content that call out blind spots in government policies and to intimidate and prosecute these content creators through hefty fines and jail time. Efforts to hold political office holders and government officials accountable for their policies are increasingly penalised.

These government actions have significantly impacted civil society actors in numerous ways. First, individuals and organisations utilising the online sphere to hold government officials and policies accountable have come under intense scrutiny, resulting in the criminalisation of critics and the blocking and removal of online content deemed sensitive by state authorities.

Second, the effectiveness of civil society in holding governments accountable is compromised, as state authorities routinely direct internet service providers and technology companies to block or remove online content considered sensitive or illegal. Consequently, individuals and organisations increasingly find their digital content at risk of being blocked or removed, succumbing to government directives to internet service providers and technology companies. This diminishes civil society's calls for accountability.

Third, on several instances, governments have imposed internet shutdowns - particularly during elections and politically sensitive periods - to disrupt the information flow. Ultimately, this has limited civil society's ability to send and receive communications effectively to mobilise people to hold governments publicly accountable during politically important instances.

Fourth, trolling has surfaced as a mainstream strategy to harass and intimidate individuals and organisations who seek to hold governments accountable. Typically orchestrated by organised groups or cybertroopers, these digital attacks increasingly involve online hate speech directed at women who call out blindspots in government policies.

Fifth, the ways of working of INGOs and CSOs have changed, leading many organisations to restrict the scope and assertiveness of their communications to shield themselves from government retribution and trolling. Some entities have opted to remove the visibility of their organisations, incorporating measures such as disallowing the use of their logos or the publishing of videos, photos and text by local partners in order to distance themselves from particular activities and contents of knowledge products.

Given these developments, the principal recommendation is that key stakeholders, including international organisations, governments, ISPs and technology companies, and civil society actors, should recognise that criticism of government policies and officials is a legitimate activity and a vital form of expression for civil society. Hence, any measures, whether legal or non-legal, that interfere with or criminalise this legitimate activity should be rescinded or disallowed. Instead, measures should be put in place to ensure that civil society is empowered to call out the blind spots in government policies.

To implement this key recommendation, collaborative efforts are needed to ensure that civil society's ability to call out the blind spots of public policy is upheld. Online content regulations should not undermine civil society's capacity to hold governments accountable.

1. Introduction

This report reviews the legal frameworks enacted by governments in the Asia-Pacific region to regulate online content. In short, it shows that online content regulations in the region have decreased civil society's ability to keep governments publicly accountable. The first chapter highlights the evolution of the region's communications landscape and how this has been leveraged by civil society for advocacy. The second chapter examines the suite of laws, such as penal codes and national security laws, alongside internet-specific regulations like fake news and cybersecurity laws and controls over internet service providers and technology companies. The third chapter analyses the negative impact of these laws on civil society, resulting in their weakened ability to hold governments accountable. The report concludes with policy recommendations directed to ensure that civil society's ability to hold governments publicly accountable is not compromised.

1a. Methodology

In preparing this report, the Asia Centre research team undertook desk research between November 2023 and January 2024. During this period, the team reviewed legal provisions shaping the digital sphere in Asia-Pacific countries and analysed how they impact civil society. The research also included a review of reports published by international non-governmental organisations (INGOs) as well as news reports from both local and international media that examined legislation that impacted the activities of civil society in the region. The research team also consulted Asia Centre's corpus of publications on internet freedoms: *Digital Security and Human Rights Defenders Landscape: Recommendations for NHRIs in the Asia-Pacific* (2023), *Digital Security and Human Rights Defenders in the Asia-Pacific* (2023), *Political Hate Sites in Singapore: Flourishing without Repercussions* (2023), *Internet Freedoms in Malaysia: Regulating Online Discourse on Race, Religion, and Royalty* (2023), *Internet Freedoms in Thailand* (2022), *Media Freedom in Southeast Asia: Repeal Restrictive Laws, Strengthen Quality Journalism* (2022), *Internet Freedoms in Cambodia: A Gateway to Control* (2021), *Myanmar: Dismantling Dissent: Crackdowns on Internet Freedoms* (2021). Versions of the draft report were internally reviewed following Asia Centre's institutional processes, incorporating feedback and suggestions into the final document.

1b. Definition of Key Terms

To assist readers in understanding the report and the key terms used, the following definitions are provided and explained here.

Content Regulation: an existing law or series of laws used in each country to deter or dictate content legally permissible to be published over traditional mediums as well as published or shared over the internet, social media platforms and messaging applications

Civil Society Organisations (CSOs): independently constituted non-governmental organisations, foundations, social enterprises as well as not-for-profit business entities that advocate for particular causes often calling out the policy lapses of governments.

International Non-Governmental Organisations (INGOs): not-for-profit organisations that advocate for a particular cause and operate globally. They work both directly and in partnership with regional and national CSOs to extend the reach of their work.

Independent Media Organisations: refers to any media – such as television, public broadcasting, newspapers, news agencies, and online outlets – that are not subject to government or corporate interests and funding, and based their reportage on journalistic ethics and standards.

Political Office Holders, Government Officials and Public Policy: political office holders are individuals who hold executive positions in government responsible for making public policies, while government officials are those responsible for implementing them. Public policy is a set of laws and processes to achieve a particular social outcome.

1c. The Digital Communications Landscape

Since the early 2000s, the digital landscape in the Asia-Pacific region has experienced remarkable growth, ushering in unprecedented speed in digital connectivity. The use of digital tools has been integrated into the daily lives of millions across the region, enabling individuals to become content creators themselves. As these technologies continue to reshape communication and information dissemination, countries in the Asia Pacific have found themselves at the forefront of a digital revolution where there is a battle to control the creation and dissemination of content to shape narratives over digital platforms.

The Asia-Pacific region has witnessed a substantial surge in internet usage in the 2010s. As of 2022, the average internet penetration in South Asia, Southeast Asia, and East Asia had reached 42.59%, 85.17%, and 83.58% of the total population in their respective sub-regions (World Bank, 2023). For reference, in the same year, the highest internet penetration indices were found in Northern Europe (97.4%), Western Europe (93.5%), and North America (92%) (Kemp, 2023a). In the Asia Pacific region, these internet penetration indices represent a significant shift from a decade ago in 2013, when the same indices were at 11.3%, 40%, and 42% relative to the sub-region's population (World Bank, 2023).

Table 1: Internet Penetration, 2013 and 2022
(World Bank, 2023)

Region	2013	2022
South Asia	11.3%	42.6%
East Asia	42%	83.6%
Southeast Asia	40%	85.2%

The surge in internet usage has become notably apparent across three key dimensions, elucidated as follows: the widespread adoption of social media platforms, the expansion of messaging applications, and the burgeoning opportunities for user-generated content creation and dissemination.

Regarding social media usage, the statistics as of 2023 indicate that approximately 32.5% of South Asia's population engages with social media (Kemp, 2023b). The distribution of the most utilised social media platforms per the local populations in the region is as follows: Facebook dominates in Bangladesh (25%) and Nepal (38.6%), Instagram takes the lead in India (74%), and YouTube holds sway in Pakistan (30%) and Sri Lanka (32.2%) (Ibid).

In early 2023, in Southeast Asia, 63.7% of the total population were social media users (Kemp, 2023c). The popularity of social networking sites began with Facebook's rapid widespread popularity in the early 2010s, when Indonesia, India, Malaysia, Philippines, and Thailand were ranked as the top ten fastest-growing markets for the firm (Tech Wire Asia, 2010). Across the ten nations, except Brunei and Indonesia where Instagram secured the first place, the most used platform is still Facebook (Cambodia, Laos, Philippines, Malaysia, Myanmar, Singapore, Thailand and Vietnam) (Kemp, 2023b).

Table 2: Most Popular Social Media Platforms in the Asia-Pacific
(Compiled by Asia Centre)

Region	Social Media Platform	Countries
South Asia	Facebook	Bangladesh and Nepal
	YouTube	Pakistan and Sri Lanka
	Instagram	India
Southeast Asia	Facebook	Cambodia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam
	Instagram	Brunei and Indonesia
East Asia	Facebook	Taiwan
	Instagram	South Korea
	Twitter	Japan

However, starting in 2018, the dominant position of Facebook and Instagram was increasingly challenged by TikTok, which became the most downloaded app in 2021 and 2022 globally (Koetsier, 2023). In 2023, in Southeast Asia, TikTok was the second-most popular social media app in Cambodia, the Philippines, Thailand and Vietnam and the third in Indonesia, Malaysia and Singapore (Kemp, 2023b). The sudden popularity of TikTok has raised concerns as China has used the platform as part of its overseas influence operations (Hale, 2023). Five out of ten Southeast Asian countries are ranked in the top ten being at risk from the malign influence of digital authoritarianism coming from China (DoubleThink Lab, 2022).

As of 2023, approximately 72% of the East Asian population actively engaged with social media. The predominant social media platforms in the region were Facebook in Taiwan, Instagram in South Korea, and Twitter in Japan (Kemp, 2023d). Drawing parallels with Southeast Asia, TikTok is gaining prominence as an emerging social media application in East Asia, ranking third in South Korea and Taiwan, and fourth in Japan (Ibid.).

Table 3: Share of TikTok Users in Asia-Pacific Countries
(DataReportal, 2023)

Country	TikTok Users (million)	Users compared to population
Indonesia	113	40.8%
Vietnam	50.58	51.3%
Philippines	41.43	35.4%
Thailand	41.07	57.2%
Pakistan	27.55	11.5%
Japan	21.07	17.1%
Malaysia	20.08	58.7%
Cambodia	7.42	43.9%
South Korea	5.47	10.6%
Taiwan	5.38	22.5%
Singapore	2.51	41.8%

In terms of messaging applications in the Asia-Pacific region, three major contenders stand out: Facebook Messenger, WhatsApp, and LINE. In South Asia, WhatsApp is exclusively favoured in India, while other countries lean towards Facebook Messenger. Southeast Asia exhibits a division with Facebook Messenger dominating in Brunei, Cambodia, the Philippines, and Vietnam; WhatsApp leading in Indonesia, Malaysia, and Singapore; and LINE being the preference in Thailand. In East Asia, excluding South Korea where KakaoTalk takes precedence, LINE emerges as the most popular messaging app in Japan and Taiwan (Ibid.) In China, the most used messaging platform is WeChat with an estimated 827.2 million users (Shewale, 2023). It is noteworthy to observe the growing impact of China's messaging app WeChat, especially in Southeast Asian countries with significant overseas Chinese communities like Malaysia, Singapore, and Thailand (Kao, 2023).

Table 4: Most Popular Messaging Applications in the Asia-Pacific
(Compiled by Asia Centre)

Region	Social Media Platform	Countries
South Asia	Facebook Messenger	Bangladesh, Nepal, Pakistan and Sri Lanka
	WhatsApp	India
Southeast Asia	Facebook Messenger	Brunei, Cambodia, Philippines and Vietnam
	WhatsApp	Indonesia, Malaysia and Singapore

Region	Social Media Platform	Countries
	LINE	Thailand
	WeChat	*Chinese-speaking communities in Malaysia, Singapore, Thailand*
East Asia	LINE	Japan and Taiwan
	KakaoTalk	South Korea
	WeChat	China

Against this backdrop, the popularity of the internet and online media content has altered the role of traditional media like newspapers and radio stations. This is discussed in the next section.

1d. Changed Patterns of Information Consumption

The 2023 Digital News Report from the Reuters Institute for the Study of Journalism (2023) highlights a significant shift in news consumption patterns, indicating a growing reliance on online sources, often emanating from non-traditional media entities, including social media. According to the report, an average of 80% of respondents in Asia-Pacific countries now turn to online sources as their primary avenue for news consumption. In contrast, only 50% and 20% of respondents opt for TV and print media, respectively. This underscores the increasing dominance of digital platforms in shaping the news landscape across the region.

The advent of digitalisation, coupled with the widespread accessibility of news content through mobile devices, has rendered traditional print media obsolete and economically burdensome. Media outlets, grappling with monthly fixed costs like staff salaries, equipment fees, and office rents, have faced the need for adaptation. In response, some media entities have sought to navigate this landscape by transitioning to online platforms. They often implement a subscription model, requiring readers to pay for access to what is marketed as "high-quality, premium content" or they resort to aggressive advertising strategies. This shift reflects a broader industry trend towards leveraging the digital realm to sustain news dissemination in a financially viable manner.

However, this strategy presents some challenges since not all readers may be incentivised to pay for content. On the other hand, news reporting and analysis by alternative media or everyday citizens is cost-free and easily accessible. Most importantly, it is often regarded as independent from the interests of private corporations and governments.

Social media platforms also make interaction between content creators and audiences easier. Known as user-generated content (UGC), social media and messaging applications, in particular, have led to the growth of online content created by people themselves rather than legacy media or other media production houses. This has scuttled the dominance of traditional media as a source of information as UGC has become the preferred choice for its speed, diversity and authenticity.

Content creators can build meaningful relationships with their audiences through various tools and styles of storytelling (Piga, 2022). For example, short video features have enabled individuals to become content creators or citizen journalists with ease and their stories more engaging compared to traditional reportage with a strict editorial line and time-consuming production stages. In other words,

new forms of creating and sharing information have emerged and are challenging traditional news reports as sources of news consumption.

Another factor that has accelerated user-generated content is the declining trust in media. According to the Reuters Institute for the Study of Journalism (2023), public trust in the media in Asia-Pacific countries is relatively low, ranging from 38% to 45% on average, with South Korea (28%), Taiwan (28%) recording lower than average trust in the media. The diminished trust can be attributed to the widespread practice of self-censorship or alignment with government agencies and corporate interests among most media outlets in the region (Dien, 2022). This climate prompts individuals to seek alternative sources of information and news.

This change in information production and consumption positively enhanced the advocacy work of civil society and CSOs in the early days, creating a wide range of new opportunities to engage with the public more effectively and efficiently. This and other examples are discussed in the next section.

1e. Digital Tools for Advocacy

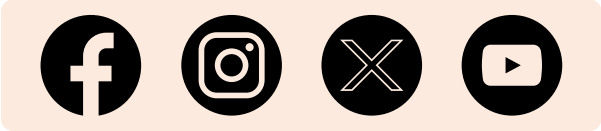
Some non-state actors immediately saw the benefits of a decentralised information architecture brought about by social media and other digital tools to boost their advocacy efforts or to mobilise individuals for social causes (USAID, 2014). As a result, social media platforms and messaging applications became powerful tools for activists and individuals interested in social actions to expand the reach of their key arguments, mobilise support, and deepen connections between local and global communities.

Enhanced methods for content dissemination have provided a pivotal advantage for civil society. Leveraging digital tools, CSOs expanded their outreach through various social media channels, encompassing platforms like Facebook, Instagram and Twitter. This was particularly valuable when disseminating news or coordinating protests (Ghonim, 2012). The existence of private groups within these social media platforms further fostered an environment where individuals felt more at ease discussing sensitive issues and exploring new ideas. A noteworthy example of this is the 2013 general election in Cambodia, where social networking platforms like Facebook played a significant role in reshaping social and political dynamics. These platforms facilitated public discussions on political matters and encouraged greater direct involvement of the public in political processes (Kimseng, 2014).

Furthermore, the digital landscape enabled the virtual hosting and broadcast of previously exclusive onsite events like roundtable discussions or workshops. Platforms such as Facebook Live offer built-in features for real-time dissemination, while recordings of these events can be uploaded onto the CSOs' or INGOs' YouTube channels for subsequent promotion. This integration of social media not only fosters inclusivity by highlighting often-overlooked narratives but also provides a versatile platform for the advocacy and promotion of social causes. The 2022 ASEAN Youth Forum exemplified this point when it hosted virtual workshops and discussion panels on lesser-discussed topics such as climate change and mental health by using Zoom and Facebook Live to reach a wider audience across Southeast Asia (ASEAN Youth Forum, n.d.).

The widespread adoption of social media has played a crucial role in amplifying and liberating voices that were often kept marginalised, by establishing new connections between underrepresented communities, CSOs, and the broader public. Elevating the visibility of these voices through social media platforms enabled the direct sharing of lived experiences related to discrimination, income

disparity, and the absence of access to fundamental infrastructure from the marginalised individuals themselves. The rise of social media empowered Dalit[1] communities in India to challenge the status quo and advocate for their rights. For example, the rights group Bhim Army effectively utilised social media to mobilise protests, share updates, and organise communities, particularly during instances of caste-based violence (Kulshreshth, 2023).



Given their ability to reach larger audiences through information sharing, social media platforms and messaging applications enable individuals and groups to organise solidarity actions or protests in the real world around social causes. Two messaging platforms stand out for political activism due to their emphasis on user privacy: Telegram and Signal. Both are open-source platforms where users can check their programming codes whether they contain features that collect users' data without prior consent. Disappearing messages – which allow users to set a timer on the messages when they will disappear – is a feature integrated into both apps. In June 2020, Signal went further to roll out a new feature that can blur people's faces in the photos of public gatherings (Perrigo, 2020).

When operating in a relatively closed civic space, Facebook pages and Twitter accounts can be used to coordinate the locations of demonstrations and provide instructions or cautions for protesters on a real-time basis. The ability to shift locations or organise a flash mob and quickly disperse put authorities at a disadvantage as the latter needed more time and approval from their superiors to move heavy equipment such as protective gear and vehicles needed to disperse the crowd.

Certain features on social media platforms facilitated direct advocacy by CSOs and community organisers with public office holders, including senators and legislators. In countries like the United States, such features enable users to identify, follow, and directly engage with lawmakers at various levels who have Facebook pages. In contrast, in Asia, social media is predominantly utilised for advocating against corruption. An example is the 2019 Indonesian youth-led campaign, #ReformasiDikorupsi (reform corrupted), which utilised Twitter and Facebook to expose corruption scandals, rally public support, and engage directly with officials. This campaign played a pivotal role in pressuring lawmakers to pass anti-corruption legislation in Indonesia (The Jakarta Post, 2019). In South Korea, CSOs leveraged Twitter and Facebook to orchestrate extensive protests against President Park Geun-hye in 2016, ultimately resulting in her impeachment and removal from office (Kim, 2016).

Increased internet, social media and messaging application usage to hold the government accountable for their public policies has challenged the hegemony of long-standing ruling families, political parties and military regimes. As a consequence, governments have begun a trend of introducing online content regulations to reel in criticism of government policies and officials. The next chapter provides an overview of the key trends to date.

[1] Members of the lowest caste in the Hindu-based social hierarchy who are marginalised in South Asia, particularly in India, Nepal, Pakistan and Bangladesh.

2. Online Content Regulations in the Asia-Pacific

In the Asia-Pacific region, governments are using legal provisions to reel in civil society's increasingly effective use of digital tools to hold political office bearers, government officials and policies publicly accountable. This chapter presents five types of laws: penal codes and national security laws, electronic and computer usage laws, fake news laws, laws on internet service providers (ISPs) and social media platforms, and laws on internet infrastructure. The laws presented in this chapter can be categorised into two groups. The first one, encompassing penal codes and national security laws in the first section of this chapter, represents pre-internet legal provisions that are still being used to govern the digital sphere. The second group of laws - the remaining four sections - are cyber laws or laws drafted and enacted specifically to regulate the digital sphere. The use of all these laws constitutes the internet regulatory framework.

2a. Penal Codes and National Security Laws

In South and Southeast Asia, penal codes originating from colonial-era legislation were initially employed to manage local populations and ethno-religious tensions. Specifically, sedition and defamation laws were utilised to prevent public communication from sparking civil unrest or uprisings against colonial rule. Post-independence, however, national leaders continued to adopt a similar approach, wielding penal codes to criminalise publications or verbal expressions deemed false, inflammatory, or critical of the governments (Asia Centre, 2020). The absence of alternative legislation led to the continued use of these colonial laws, especially in managing diverse, multi-religious, and multi-ethnic societies.

In South Asia, Bangladesh, India, Nepal, Pakistan, and Sri Lanka are former colonies of the British Empire. This means they share the same jurisprudence deriving from the Indian Penal Code (1860). Following independence, these territories have continued to use the same law to solidify the efforts to build a homogenous national identity and safeguard the independence from ethno-religious strife that might derail the nation-building process (Asia Centre, 2020). Such differences include the antagonism between Hinduism and Islam (Bangladesh, India, Pakistan), or racial conflict between the Tamils and Sinhalese (Sri Lanka). These laws have therefore been justified to quell activities that authorities deem perpetuating ethno-religious conflict. In the same vein, In 2015, the Sri Lankan government sought to amend the penal code to indicate the penalty for hate speech, arguing the need for a legal response against racial violence in the country (Gunatilleke, 2016).

With the coming of the internet in the late 1990s, the application of the Penal Code has gradually changed, extending the prohibitions to online content, messages and discussions and online publications and social media platforms. At the time, some countries (Bangladesh, Nepal, Sri Lanka) have stuck to this legal approach using the Penal Code or national security-related laws (Freedom

House, 1999). Others (India and Pakistan) have gradually moved on to computer usage or social media laws as their Supreme Courts have either repealed or put a moratorium on sedition offences.

In Southeast Asia, Brunei, Malaysia, Myanmar, and Singapore directly inherited the Indian Penal Code, though they passed separate, stand-alone Sedition Act or Public Order Act – with provisions taken from India's Code. Indonesia has been using the colonial-era Penal Code, promulgated by the Dutch in 1918. Although the new indigenous Penal Code was introduced in December 2023 and to be effective in 2026, the Code retains defamation provisions from the colonial version. Due to their Indian roots, the criminal codes of respective countries have similarly been used to manage ethno-religious tensions. For example, in Singapore, the police regularly arrest individuals making racist remarks online by invoking Section 298A of the criminal code regarding statements wounding "religious or racial feelings" (Singapore Police Force, 2020). Such use of criminal code can also be found in Myanmar, where Section 295A (outraging religious feelings) is regularly invoked (Asia Centre, 2021b).

Cambodia, after emerging from a civil war, received technical assistance from French officials when drafting its own Penal Code (2001). Its Section 495 on incitement to violence, has been used against reporting by online independent journalists seeking to shed light on the government's policy mismanagements (Hul, 2020). Meanwhile, Laos and Vietnam achieved independence through communist revolutions. As part of the efforts to consolidate power after the revolution, these countries introduced a Penal Code with provisions prohibiting propaganda against the state (Article 117 of respective Codes) to curb perceived dissent against respective communist governments (Gomez & Butrkrawee, 2023).

Thailand is a unique case because it has never been colonised by Western powers. Still, the country's Penal Code (1956) contains lèse-majesté offence (Article 112) and sedition offence (Article 116) to preserve the revered status of the monarchy in the society, which various administrations deem inseparable from national security and public order. The amendment to Article 112 – increasing the maximum imprisonment term to 15 years – after a massacre to suppress a potential communist uprising in 1976 reflected this state ideology. Similarly, in 2018, Cambodia revised its Penal Code to add lèse-majesté as a punishable offence (Thul, 2018). Starting in 2019, Malaysia has used the lèse-majesté offence under the Sedition Act to deter members of the public from criticising the monarchy (Barrett, 2021).

In East Asia, given their homogenous population and exposure to democratic values and practices, Articles 230 and 233 of the Japanese Penal Code, Article 304(2) South Korean Penal Code and Article 313 of the Taiwanese Penal Code have rarely been used to deter political expression or the spread of hate speech and false information. Rather, they prefer the media to regulate themselves or in the case of South Korea refer the case to the Press Arbitration Committee. Taiwan has started to amend its Penal Code to criminalise disinformation, though only after China became more assertive and engaged in overseas influence operations against Taiwan (Department of Information Services, 2019).

Except for East Asia, early in the era of internet usage, provisions within penal codes aimed at preserving public order and safeguarding the reputation of public officials or the head of state were utilised to control online discussions and content. While most countries transitioned to electronic or computer usage laws, some nations in the Asia-Pacific region persist in resorting to penal codes to regulate online content and behaviours.

2b. Electronic and Computer Usage Laws

When internet penetration started to take hold in the Asia-Pacific, there were two main factors influencing governments' decision to enact legal measures limiting online communication, particularly in South and Southeast Asia: terrorism in South Asia and increased demands for public accountability in Southeast Asia. Notably, East Asian countries opted for a more restrained approach, adhering to a self-regulatory regime.

In the context of South Asia, post-colonial border alignments paved the way for the emergence of national sentiments driven by political aspirations for autonomy. This dynamic led to acts of violence associated with religious extremism, rooted in specific ideological interpretations, and ethno-nationalist separatist movements fuelled by grievances related to ethnicity or language (Priva, n.d.), marking them as national security concerns. However, a crucial turning point occurred with the events of 11 September, reshaping the narrative to spotlight terrorism. This shift empowered South Asian governments to categorise the mentioned groups as terrorists, allowing the application of legal provisions to prevent their actions.

Instances when terrorists have made use of the internet to either spread extremist materials or facilitate their operations include the 2014 Peshawar Terrorist Attack (Pakistan) and the 2016 Dhaka Terrorist Attack (Bangladesh). The timing of Pakistan's Prevention of Electronic Crimes Act (PECA) (2016) and Bangladesh's Digital Security Act (DSA) (2018) coincided with the rise of the Islamic State of Iraq and Syria starting in 2014. PECA, for example, was introduced as part of the government's 20-point action plan against terrorism (Arshad Khan, 2016). However, provisions were expanded to cover criminalising comments considered by authorities as "hate speech" or "anti-state" behaviours (TrialWatch, 2023). In a similar context, the DSA included provisions against cyber terrorism, albeit with a limited explanation of what "terrorism" delineates (OHCHR, 2022).

The emergence of the internet in Southeast Asia ushered in a transformative period, allowing opposition parties and civil society groups to increase their demands for public accountability from governments. As a result, In this region, governments exercised significant control over online channels, amending and introducing new print and broadcast laws to regulate the online activities of the members of these groups demanding public accountability. Malaysia and Singapore were the first to introduce online content regulations and media licensing regimes through the Broadcasting Act (Singapore) (1994) and Communications and Multimedia Act (1998). Others, as explained next, opt for electronic transaction laws or computer/cybercrime acts, which contain vaguely worded provisions that can be used to criminalise content deemed false or affecting public or ethno-religious harmony.

In Thailand, the junta heavily controlled traditional media after the 2014 coup, making it difficult for dissenting voices to be heard. Opposition groups and activists turned to online platforms like Facebook and Twitter to share their messages and mobilise supporters. The online Red Shirt movement, advocating for ousted Prime Minister Thaksin Shinawatra, emerged largely through social media, organising protests and disseminating information beyond state censorship (Feldstein, 2021). Enacted in 2007 and subsequently undergoing multiple amendments, particularly post the 2014 coup, the Computer Crime Act (CCA) in Thailand encompasses crucial provisions relevant to online activism. Additionally, Article 14(2) prohibits the creation or dissemination of "false information" that might incite public panic or jeopardise national security, with a broad application against online activism.

Myanmar's ethnic minorities, particularly the Rohingya, faced historical oppression, but the internet briefly offered a platform for sharing human rights abuses and demanding public accountability. Using

social media, the Rohingya documented their plight, connecting with global audiences and advocating for justice. However, Myanmar's government responded harshly with the Cybercrime Law (2022), imposing prison sentences for online dissent. Mass surveillance and social media bans during unrest further restricted expression. Online activists endure harassment and imprisonment, creating a chilling effect on digital advocacy.

As the examples from South and Southeast Asia show, legal frameworks governing online communication in the Asia-Pacific region have undergone significant changes, driven by factors such as nationalist and separatist movements arising from post-colonial border re-alignment were labelled terrorism following the jargon of 11 September. The surge of social media has prompted the introduction or amendment of laws dealing with issues like fake news and online hate speech. In contrast to that, East Asian nations have largely leaned towards self-regulation in addressing these challenges. This nuanced regional approach reflects the diverse strategies employed in the Asia-Pacific region to navigate the complex landscape of online communication regulations.

2c. Fake News Law

In the late 2010s, social media and messaging applications became popular platforms for online discussion, activism and advocacy. But fake news, hate speech and disinformation also become widespread through these services. In some instances, these have affected the functioning of domestic democratic institutions or practices such as elections or referendums (Asia Centre, 2022b; Asia Centre, 2023b). While the threats are real, authorities in the Asia-Pacific region have allegedly taken advantage of the situation to pass fake news legislation to counter online disinformation and hate speech, but also to control online content that is critical of the governments and deemed "fake".

In South Asia, attempts to enact "fake news" laws emerged as a result of increased hate speech and communal tensions across religious and ethnic lines. In particular, the justification given was to protect against sectarian groups that exploit ethno-religious tensions within society to disseminate false information to gain wider attention or reach (Janjua 2022, Livelaw, 2023). In August 2023, the Prohibition of Fake News on Social Media Bill (2023) was introduced to the Indian parliament and is currently under review. In 2022, the government of Pakistan tried to pass amendments to PECA to combat fake news. However, intervention from the High Court and pushback from the media led to the government changing course. Similarly, the ethno-religious tension following the Easter Sunday Bombing (2019) has convinced Sri Lanka to come up with an online content regulation, although the legislation has never proceeded beyond the draft stage (Angwalkar, 2021).

In Southeast Asia, by the late 2010s, social media platforms and messaging apps have become either a public space for citizens to voice their concerns or criticism over policy gaps directed at public officials. This development has led Indonesia, Myanmar, and Thailand to amend their existing laws (UU ITE (2016), Electronic Transaction Law (2021) and Computer Crime Act (2017) to take action against critical online content framed as false information or defamation. On the other hand, Malaysia and Singapore, again, took the lead in the region in legislating specific fake news laws, citing disinformation during election periods. Malaysia's Anti-Fake News Act (2018), though later repealed in 2021, served as an impulsion for Singapore to come up with its fake news legislation – the Protection from Online Falsehoods and Manipulation Act (POFMA) (2019).

In East Asia, the fear of disinformation being used by China to conduct overseas influence operations has led lawmakers in South Korea and Taiwan to propose fake news laws. In the case of South Korea, the parliament, in 2021, tried to pass an amendment to the Act of Press Arbitration, which would add

provisions related to mis- and disinformation. Due to critical responses and concerns regarding freedom of expression, the bill was shelved (New Sang-Hun, 2021). Japan remains firm in using non-legal measures such as fact-checking or allowing the media to regulate themselves when confronting the issue of disinformation. The commitment towards a non-regulatory approach within these societies prevailed and no legislation was passed.

All in all, what is observed is that, in practice, the implementation of fake news laws often takes a turn. Rather than solely targeting misinformation, these laws are frequently used against civil society actors, opposition party leaders and independent journalists who aim at holding governments accountable to the public. This trend underscores the challenges and complexities surrounding the actual application of such regulations in the context of political dynamics in the region.

2d. Laws on Service and Digital Platforms Providers

As has been shown in the previous section, legal frameworks like Singapore's POFMA and Thailand's Computer Crime Act already incorporate provisions addressing service and platform providers, in addition to individual liability. In contrast, countries like India, Indonesia, Nepal, Pakistan, and Vietnam are anticipated to introduce new, dedicated laws compelling ISPs and social media companies to adhere to their notice-and-take-down requests in due course. This section delves into the details of laws governing service and platform providers.

In the 2010s, South and Southeast Asian states became aware of their influence over ISPs and technology companies that provide social media and messaging application services due to the expanding population and advertising revenues (Timmerman, 2022). This realisation prompted governments to modify existing laws or enact new ones, incorporating specific provisions directed at service and platform providers. Notably, a prevailing trend is the requirement for social media firms to register with pertinent government agencies, with the consequence of potential business closure for non-compliance.

In South Asia, after the sedition offences under the Penal Codes were repealed or suspended, India and Pakistan have legislated laws that directly target ISPs and technology companies to enforce notice-and-takedown orders. For this reason, Pakistan passed the Removal and Blocking of Unlawful Online Content Rules (2021) (The Rules) adding financial liability on technology companies that do not observe takedown requests from the government (Amin, 2021). In 2023, India amended the Information Technology Rules (2021) to obligate social media intermediaries to observe content removal requests or lose immunity from civil and criminal liability for the content created or shared on their platforms (Global Network Initiative, 2023). Nepal followed the trend in November 2023, introducing Directives on the Operation of Social Networking (The Kathmandu Post, 2024). Aside from takedown requests, the law necessitates social media platforms to register with the relevant state agency and set up a local office, or risk a shutdown of the platform (Ibid.).

In Southeast Asia, three actions against ISPs and technology companies are adopted: business closure, hefty fines and liability for criminal offences. Due to the fear of being forced to shut down their operations, ISPs and social media platforms signed up to the registration regime of Indonesian Ministerial Regulation No. 5 (2020), which requires them to take down prohibited content believed to be violating the country's law or disturbing public order (Telling & Criddle, 2022). A similar approach to business closure was also officiated under Vietnam's Decree No. 53/2022/ND-CP (2022). As the Decree requires ISPs and social media platforms to remove content, failure to comply will result in service suspension or termination.

Singapore, through POFMA, pursues a hefty fine regime towards ISPs and technology companies. Failure to comply with a correction order or denial-of-service order will result in a fine of as much as US$ 372,630. Furthermore, if they fail to observe the POFMA Code of Practice on political advertisement, a fine of up to US$ 745,260 could be imposed. In Thailand, per the Computer Crime Act, criminal liability is used to pressure ISPs and social media service providers to remove content deemed affecting national security. This could be up to 15 years imprisonment if the concerned content is lèse-majesté.

In East Asia, Japan and South Korea have legislation requesting service providers to remove content. In April 2021, Japan amended the Provider Liability Limitation Act to allow online users – when the infringement of their rights is evident and justifiable – to request disclosure of the IP address of the offender from the ISP, or demand removal of concerned content or information, or make claims for tort damages from the offenders (Kobayashi, 2022). In South Korea, the Korean Communications Committee and the Korean Communication Standards Committee regularly issue orders for ISPs to block or delete content from the internet, that, among other justifications, are defamatory, in praise of North Korea, and anti-military (Yoon, 2017).

To sum up, the legal frameworks discussed here underscore a pattern. Laws targeting service and platform providers, such as Singapore's POFMA and Thailand's Computer Crime Act, are increasingly employed not just to combat misinformation but also as tools against those seeking public accountability or simply expressing different views on such policies.

2e. Internet Infrastructure Laws

In South and Southeast Asia, a practice that is becoming a trend is the imposition of internet shutdowns during periods of heightened political activities such as protests, unrest or elections that bring together many individuals and activists seeking greater public accountability. These incidents usually occur in regions or localities where conflicts or tensions are simmering, including the Thai Deep South, Mindanao in the Philippines, or Myanmar, where many ethnic groups are seeking greater autonomy or independence. This represents a shift away from trying to control online content, or individuals from publishing information considered false, or critical of the government, towards controlling or disabling internet infrastructure entirely. Apart from China, such developments have not been found in East Asia.

In 2022, according to Access Now's #KeepItOn report South Asia led the world in internet shutdown with India imposing a total of 84 internet shutdowns, followed by Bangladesh (7) and Pakistan (1) (Access Now, 2023b). In India, the service shutdown is imposed through Section 144 of the Penal Code and the Temporary Suspension of Telecom Services Rules (2017). In Bangladesh and Pakistan, Telecommunications Acts (Bangladesh (2001) and Pakistan (1997)) are the main legal instruments used to suspend internet service. While most internet shutdowns were taken to prevent communal, sectarian violence, instances in Bangladesh and Pakistan suggested that it was allegedly used to disrupt political opponents from organising political rallies (Newage BD, 2024).

In Southeast Asia, internet shutdowns have been primarily taken by Myanmar and Indonesia. The aim is to curb political activism and deny them access to the internet and social media, which could be used for political mobilisation. Following the coup in February 2021, the Myanmar military junta used Section 77 of the Telecommunication Law (2013) to impose a nationwide internet shutdown to prevent resistance from the population (Reuters, 2021). This was on top of what experts considered the world's longest internet shutdown in the Rakhine and Chin areas, where armed conflicts between the ethnic groups and government forces were undergoing (Hlaing, 2021). In Indonesia, the UU ITE was used to

enact internet service suspension in the restive province of West Papua, where separatism has been brewing. In 2019, at least three rounds of internet shutdowns were enforced in the province (Access Now, 2023a).

On the other hand, Cambodia has a different way of imposing control over internet infrastructure. In 2021, Cambodia passed the Sub-Decree on National Internet Gateway (NIG) (2021). Rerouting internet activity and web traffic through a single regulated node makes it easier for the government to disrupt or disconnect online connections and impose nationwide state surveillance. Originally, the idea of an internet gateway was first floated by Thailand's military junta in 2015, after they staged a coup, to narrow down various internet gateways into a single, national gateway. The plan was shelved, however, due to pushback from civil society (Reuters, 2015).

China's Great Firewall, also known as the Golden Shield Project, represents a highly sophisticated internet censorship system. Governed by the Chinese authorities, it employs a combination of technical and regulatory measures to control and monitor internet traffic. This includes blocking access to foreign websites, content censorship, and surveillance of online activities. Popular international platforms like Google, Facebook, and Twitter are inaccessible, and domestic platforms are heavily regulated, reflecting the strict control exerted over digital information within China (Chew, 2018).

Broadly speaking, as demonstrated in this chapter, countries across the Asia-Pacific region have employed a wide range of legal provisions to regulate the digital sphere in response to increased and effective demands for public accountability by civil society. Governments in the region have resorted to using pre-internet-era laws, such as penal codes and national security laws, along with cyber laws that have been amended to align with the developments in the digital sphere and digital media. Laws to govern ISPs and technology companies as well as laws that allow for control over the internet infrastructure have been enacted. Of significance is how these laws have been utilised to target individuals and organisations that attempt to hold political office holders, government officials and policies publicly accountable. The next chapter of this report delves into five impacts of these laws observed in civil society.

3. Impact on Civil Society Actors

This chapter presents how governments' use of laws to regulate the digital sphere as well as their non-action towards the harassment of activists has influenced civil society's ways of working. First, how the trend of criminalising critiquing political office holders, government officials and policies has made civil society actors more cautious. Second, how internet service providers (ISPs) and technology companies are legally bound compliance to block and remove content reduces civil society's messaging and mobilisation effectiveness. Third, how politically-motivated internet shutdowns and the possible implementation of internet gateways thwart the work of civil society at politically sensitive times. Fourth, how trolls, the act of cyber-trolling and hate sites seek to actively discredit and distort the messaging of those who call out policy lapses. Finally, how these legal and non-legal measures have forced CSOs and INGOs to engage in self-inhibiting behaviours has weakened their ability to hold governments accountable.

3a. Criminalising Criticism of Government Policies

In contrast to East Asian countries, governments in South and Southeast Asia have taken advantage of online content regulations to prosecute those who call out the policy lapses of incumbent administrations. Vaguely worded laws allow government officials to selectively prosecute content producers – such as activists, media outlets and civil society organisations – for allegedly spreading disinformation or opinion that affects national security and public order whenever they call out corrupt practices of government officials or policy lapses.

Individual Activists and Leaders

Online users, civil society actors, and human rights defenders face persecution for their policy criticism when government officials accuse them instead of spreading false, illegal, and defamatory information. These accusations turn calls for government accountability into acts of disseminating fake news and spreading disinformation. Consequently, legal actions are taken, including lodging complaints and initiating court cases against activists' advocacy messages on online platforms. These legal actions are justified by alleging that activists are disseminating false information which will purportedly affect national security, public order, and social harmony. This pattern of prosecution has led to overcriminalisation as even trivial cases are pursued.

Overcriminalisation has affected some political leaders in Asia, with notable instances such as the case of Kenneth Jeyaretnam, the leader of the Reform Party in Singapore. In December 2023, the Singaporean authorities utilised POFMA to impose restrictions on Jeyaretnam. This resulted in the designation of his website and social media accounts as a Declared Online Location. Consequently, he faced a two-year prohibition from deriving any financial benefits through his online platforms. Throughout the year 2023, Kenneth Jeyaretnam encountered a series of correction directions, totalling

five instances. These corrections were in response to his comments regarding government spending, healthcare expenditure, and the perceived lack of transparency surrounding the rental of government residences by two ministers (CNA, 2023).

Other examples can be found in the news and film sectors. In 2022, Malaysian journalist Lalitha Kunaratnam was investigated under Section 233 of the Communications and Multimedia Act due to her exposé implicating Malaysian Anti-Corruption Commissioner Chief Azam Baki. In 2022, Azam took legal action against Lalitha concerning a two-part series she penned titled "Business ties among [Malaysian Anti-Corruption Commissioner Chief] leadership: How deep does it go?" The article depicted Azam as a corrupt civil servant who exploited his role as a senior MACC officer, using his position for personal gain and favouring his own or his sibling's interests. They were first released on the Independent News Service portal on 26 October 2021 and later republished on 15 December of that year. Azam also asserted that Lalitha posted links to the articles on her Twitter account (Free Malaysia Today, 2023).

In the film sector, in 2022 a Myanmar court sentenced Japanese documentary filmmaker Toru Kubota to seven years of imprisonment. The charges against Kubota were linked to his documentation of anti-junta protests, his collaboration with local activists, and his use of electronic communications technology for activities deemed threatening to state security, law and order, peace, or national solidarity. This transgression violated Section 33(a) of the Electronic Transactions Law (Myanmar Now, 2022). The aftermath of the legal proceedings saw Kubota spending three months in the notorious Insein Prison before being deported back to Japan. This case highlights the challenges filmmakers face navigating politically sensitive subject matter in regions where authorities actively silence critics.

Human rights activists who call out possible corrupt practices are also affected by the use of this legislation. A case in point was the 2023 incident involving Indonesian human rights activists Haris Azhar and Fatia Maulidiyanti. They were charged under the Information and Electronic Transaction Law (UU ITE) due to their participation in an online discussion on YouTube. In the video, they brought to light the purported involvement of senior Cabinet minister Luhut Pandjaitan in an extractive gold mining operation in Papua through his shares in the mining company PT Toba Sejahtera (Janti, 2023).

In that same year, Malaysian political activist and satirist Fahmi Reza faced legal repercussions for his policy criticism when he faced charges under Section 233 of the Communications and Multimedia Act. The charges were brought against him on two separate occasions, both stemming from his creation and online posting of satirical posters and artworks. These works targeted cabinet ministers and critiqued their controversial COVID-19 policies (CIVICUS, 2022). These examples underscore the challenging environment faced by activists who utilise online platforms to expose alleged wrongdoings where legal provisions in online content regulation laws may be employed to restrict policy criticism.

Finally, overcriminalisation also affects individuals or everyday citizens. In Thailand, spanning from July 2020 to April 2023, a total of 195 individuals were charged under the Computer Crime Act (CCA), primarily for their online mobilisation of supporters and engaging in policy criticism online. The CCA was wielded as a legal tool by Thai authorities to quell nationwide protests that began in July 2020 and the subsequent youth-led activism that followed (TLHR, 2023). The most recent court trial under the CCA unfolded in December 2023, resulting in the sentencing of activist-turned-lawmaker Rukchanok Srinork to three years of imprisonment. Her conviction stemmed from retweeting a graphic that criticised the Thai monarchy (BBC Thai, 2023).

In September 2021, Vietnamese Facebook user Nguyen Thuy Duong faced a fine of US$210 for expressing online criticism of the government's management of the COVID-19 pandemic. Her statement highlighted that lockdown measures, imposed by authorities in Ho Chi Minh City, had resulted in residents being unable to receive relief packages (RFA, 2021).

These examples show how the overcriminalisation of those who attempt to keep government officials and policies accountable poses a significant challenge in Asia, impacting a wide range of actors. Political leaders, journalists, filmmakers, activists, and ordinary citizens have faced legal actions under the pretext of combating false information and ensuring national security.

Independent Media Houses and CSOs

Like individuals and activists, some of the actions by members of independent media houses and CSOs to keep government officials and policies accountable have also been over-criminalised. This has been primarily because of the content they have published online that called out actions by public authorities.

In January 2021, Vietnamese authorities arrested Pham Chi Dung, Nguyen Tuong Thuy, and Le Huu Minh Tuan – the leadership behind the Independent Journalists Association of Vietnam – and sentenced them to 15 years and 10 years of imprisonment, effectively shutting down the association (EU, 2021). In May, another civil society organisation, Towards Transparency – the Vietnamese affiliate of Transparency International – ceased operations after the Department of Information and Communications revoked its website domain and imposed administrative fines. This action was taken after the organisation mistakenly used a regional map in its illustration of the Corruption Perceptions Index that did not conform to regulations. Governments in the region have misused these restrictions against civil society entities – especially the key management of civil society organisations and media houses, whose roles involve keeping governments accountable – with the goal of disrupting their activity.

In February 2023, the Government of Cambodia revoked the operating licence of Voice of Democracy, one of the last remaining independent media outlets in the country. The decision came after it published a news report claiming that Hun Manet – the son of former Prime Minister Hun Sen, and his political successor – had signed an aid relief agreement to donate $100,000 to Turkey, an overstep of his authority. VOD, performing an act of political oversight, called this action out. As a result, Hun Sen has accused the outlet of damaging him and his son and tarnishing the dignity and reputation of the Cambodian government (Ratcliffe, 2023).

In March 2021, one month after the coup, the Myanmar military junta cancelled the operating licences of 5 independent news media: 7 Day News, Democratic Voice of Burma, Khit Thit News, Mizzima and Myanmar Now. The government-owned television MRTV reported that these outlets are no longer allowed to publish or report news articles, and programmes, or transmit messages via their social media accounts (RSF, 2021). In 2022, another independent news outlet The Irrawaddy was shut down by the junta, bringing the total media being closed down to 20 outlets (RFA Burmese, 2021). In 2022, after being repeatedly forced to comply with Myanmar authorities to impose nationwide internet shutdowns, Telenor Myanmar decided to divest from Myanmar stating that the decision was based on their adherence to the values of human rights and responsible business, and the desire to keep their employees safe.

In September 2021, a Singaporean online media outlet The Online Citizen closed down after the Infocomm and Media Development Authority (IMDA) suspended its licence due to the former's alleged

failure to comply with legal obligations to declare all sources of funding (Kurohi, 2021). Since 2018, the TOC has faced recurrent legal actions under the POFMA and criminal defamation for highlighting deficiencies in government policy implementation, such as those related to social housing and policing.

In June 2023, the IMDA blocked access to Asia Sentinel, a California-based news website, after it published an article interviewing an author of an opinion piece in Nikkei Asia criticising Singapore's management of the COVID-19 pandemic (RSF, 2023). In September, the IMDA blocked the Australia-based academic website East Asian Forum, after it published an article criticising the lack of independence of the Corrupt Practices Investigation Bureau and the Prime Minister's management in addressing extramarital affairs among parliamentarians (Wong, 2023).

Digital communication tools have allowed independent media initiatives to report on issues related to corruption, policy lapses and the overstepping of government authorities. However, governments have responded by using laws for online content regulation to prosecute individuals seeking to keep government policies publicly accountable.

3b. Requesting Legal Compliance from ISPs and Technology Companies

Governments in the region use online content regulation laws to request internet intermediaries, including ISPs and technology companies, to block and remove content deemed illegal, sensitive, or inappropriate, which normally involves cases of corruption, overstepping of political authority, public accountability, and policies that do not take into consideration the needs of the public. This is a key strategy for governments since ISPs and technology companies exercise effective control over online content, enabling them to deny access to content as needed.

There is a recurring trend of governments issuing demands to ISPs to take action against content produced by civil society that is deemed harmful or illegal and, often, criticises government public policies and practices. While specific data on the total number of requests made by governments remains undisclosed by ISPs, news reports indicate the widespread use of such tactics, particularly in South and Southeast Asia. Independent online media and websites of CSOs have often been targeted. For instance, in India, the government issues filtering orders to ISPs to restrict access to web pages belonging to both domestic and foreign NGOs (Ailawadi, 2018). In Singapore, the government, utilising powers under the Protection from Online Falsehoods and Manipulation Act (POFMA) in 2019, directed ISPs to block access to the website of the Malaysian-based NGO "Lawyers for Liberty" due to their advocacy on prison reform in Singapore (CISOMAG, 2020). Similarly, a week before the Cambodian general election in July 2023, the government ordered ISPs to block the social media accounts and websites of three news outlets – Cambodia Daily, VOA Khmer, and Radio Free Asia (Davin & Liblib, 2023).

In 2022, to prevent the revocation of their operating licences, major technology firms like Apple, Facebook, Google, Microsoft, TikTok, and Twitter agreed to Indonesia's latest content licensing scheme. This scheme requires service providers to censor content and provide users' data upon official request (Telling & Criddle, 2022).

Governments have also been observed to make requests to technology companies to remove content that attempts to hold governments publicly accountable. Below, statistics on this matter from two technology companies, Facebook (Meta) and Google are provided.

Figure 1: Requests for Content Removal Made to Facebook

(Meta, 2023)

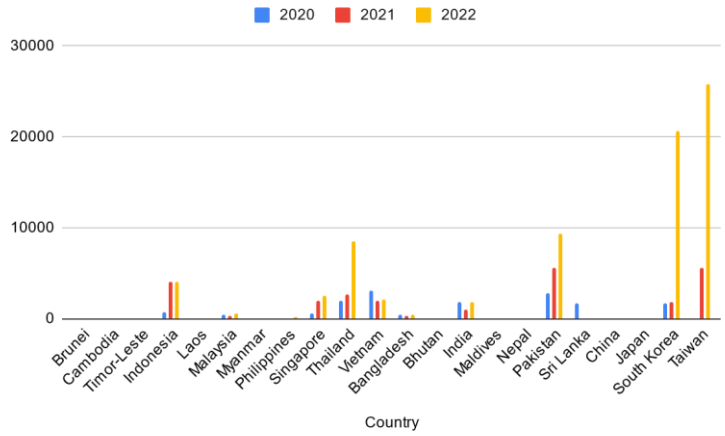
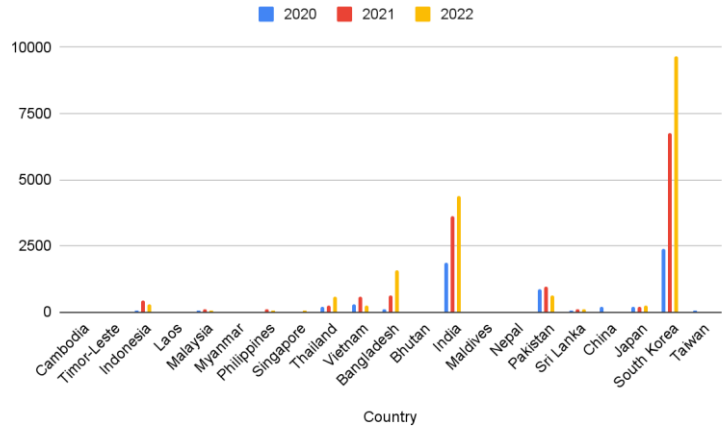


Figure 2: Requests for Content Removal Made to Google

(Google, 2023)



In Southeast Asia, there is a noticeable upward trend in the average annual content removal requests directed at Facebook (Figure 1) – particularly with substantial requests in Indonesia and a significant surge in Thailand due to, allegedly, violating local laws. The online content included government criticism and posts that called out violations of laws related to illegal gambling, hate speech, content stirring racial or religious division, instances of bullying, and financial scams (The Business Times, 2023). The regional average escalated from 618 requests to Meta in 2020 to 1,007 (2021) and 1,642 (2022). South Asia presents a varied landscape, with fluctuating trends in India, a moderate rise in Bangladesh, and a substantial increase in Pakistan, resulting in respective averages of 939 requests (2020), 981 (2021), and 1,671 (2022). East Asia exhibits diverse patterns in Facebook content removal, marked by a substantial surge in South Korea and Taiwan, and fluctuations in Japan, contributing to an average of 444 (2020), 1,900 (2021), and a notable increase to 11,626 (2022).

According to Google's data (Figure 2), Southeast Asia displays variability, with Thailand experiencing a notable surge in content removal requests, increasing from 56 requests in 2020 to 124 in 2022. In South Asia, India stands out with a significant increase, consequently raising the yearly average requests to 420 (2020), 765 (2021), and 964 (2022). South Korea exclusively contributes to an overall rising trend in East Asia, with the region seeing an increase from 701 in 2020 to over 2,400 in 2022.

Overall, Facebook and Google consistently experience a year-on-year rise in content removal requests in Southeast Asia, South Asia, and East Asia, attributed to posts considered illegal due to their content, particularly those involving hate speech or creating social divisions. While many countries do not heavily engage in content removal through these channels, countries like Indonesia, India, South Korea, and Thailand are among the highest. Notably, East Asia emerges as the region with the highest number of content removal requests, particularly on Facebook. This data underscores that the legal frameworks implemented by governments in the region empower them to compel internet intermediaries, such as ISPs and tech companies, to comply with orders to remove objectionable content.

3c. Internet Shutdowns and Internet Gateways

Internet shutdowns have emerged as contentious tools employed by governments to control information flow in the online sphere, particularly in regions experiencing political turmoil and unrest. These areas tend to be contested areas of control with strong domination by the central government and a desire for self-rule by members of religious and ethnic minorities. The shutdown in Jammu and Kashmir, India, in 2019, stands as a stark example of the impact of such measures. Following the government's decision to revoke the special autonomy status of the region by abrogating Article 370, a comprehensive communication blackout was imposed, encompassing internet and phone services. This shutdown, lasting for several months, restricted communication and access to information for the residents of Jammu and Kashmir. The blackout was gradually lifted in phases, raising concerns about freedom of expression and the right to access information (IFJ, 2020; Bhat et al., 2022).

Similarly, in Sri Lanka, the government resorted to temporary internet shutdowns in March 2018 during communal violence in the Kandy district. In Sri Lanka, a predominantly Buddhist nation, historical religious and ethnic tensions, particularly between the majority Sinhalese Buddhists and the Muslim minority, intensified leading up to the violence in Kandy. Growing tensions were fueled by issues such as alleged forced conversions and the desecration of religious sites among these communities. These above-mentioned restrictions were implemented to curb the spread of misinformation and hate speech that had the potential to exacerbate tensions within the affected region. While the goal was to maintain stability and prevent the escalation of violence, such measures also raised questions about the balance between security concerns and the citizens' right to freely access and share information (Goel et al., 2018).

After the military coup in Myanmar on 1 February 2021, the junta responded to widespread protests and civil disobedience against the coup by imposing internet restrictions. Nationwide shutdowns disrupted communication and online businesses, while social media platforms were temporarily blocked, hindering protesters' coordination. The regime used deep packet inspection technology to monitor and filter internet traffic, suppressing dissent and controlling the narrative. These measures not only hampered the flow of information but also inflicted economic damage on businesses (AccessNow, 2022), deepening the political crisis and illustrating the pivotal role of internet shutdowns in Myanmar's events.

In countries, such as Bangladesh, China, and Cambodia, the government maintains national internet gateways, centralising and controlling all international traffic to enhance authority over internet content and access.

The Bangladesh Telecommunication Regulatory Commission oversees the regulatory framework for telecommunications. The Commission has the authority to temporarily block websites and social media platforms, a measure often enacted during political unrest or security concerns. This strategic

approach allows the government to manage information flow while addressing specific situations (Biyani et al., 2021). In October 2022, it was reported that the Commission issued orders instructing mobile service operators to temporarily suspend 3G and 4G internet services in the Khulna division in anticipation of a BNP rally, one of the main opposition parties in the country (TBS News, 2022). Subsequently, in early November 2022, a similar disruption in connectivity occurred in the city of Barishal during a BNP rally, creating impediments for journalists covering the event. This sequence of events suggests a pattern of deliberate interference with communication services surrounding political gatherings (New Age BD, 2022).

In Cambodia, the government contends that the National Internet Gateway (NIG) would enhance national security efforts by providing a centralised mechanism to combat cybercrime and terrorism. Additionally, officials argue that it would enable more effective tax collection from online businesses operating within the country. Furthermore, the government asserts that the NIG would facilitate better control over online content, allowing authorities to manage information flow in a manner deemed appropriate. However, these justifications have given rise to significant concerns from various quarters. One major worry is the potential for censorship, as the NIG could provide a tool for the government to restrict access to websites and control the free flow of information. Critics also raise privacy concerns, given the government's increased control over internet traffic, which could potentially lead to extensive surveillance (Asia Centre, 2021a). As of the present, the NIG project has faced delays due to a combination of concerns and technical challenges. However, it is important to note that the project has not been officially abandoned.

The Great Firewall of China operates as a high-tech border wall, overseeing and regulating the flow of internet traffic into and out of the country. Managed by the Chinese government, particularly the Cyberspace Administration of China, it comprises a network of checkpoints employing diverse filtering techniques. These techniques include keyword blocking, redirecting users through domain name system manipulation, and conducting deep packet inspection to identify and block content based on type, format, or origin. This system has substantial impacts, rendering popular international websites like Google, Facebook, Twitter, and YouTube inaccessible within China. It also allows the government to control access to politically sensitive information, critical content, and certain ideologies, limiting access to news articles, social media posts, and academic texts - particularly those deemed as sensitive and criticising government policies and officials. In response, China has cultivated its online ecosystem with services like Baidu, Weibo, WeChat, and Youku (Economy, 2018).

To sum up, in recent years, there has been a noticeable trend of governments shifting their tactics from solely prosecuting individuals or organisations, who disseminate online content critical of public office holders and their policies, towards gaining control over internet infrastructure and empowering themselves to shut down internet service in politically sensitive periods such as protests or coup.

3d. Trolling, Cybertroopers, Hate Sites

As policy criticism and calls for public accountability against sitting administrations are being weakened, and content creators face prosecution, the internet, social media, and messaging applications have transformed into open spaces where government supporters and affiliated groups disseminate their pro-government narratives or launch attacks on political opponents, social activists, and independent journalists. Consequently, online users are increasingly hesitant to express their viewpoints openly, fearing potential targeting.

Trolling and Cybertroopers

Trolling, the act of deliberately provoking others online by posting offensive or disruptive content, is a pervasive issue affecting digital rights across Asia (Social Media Victims Law Centre, n.d.). Members of civil society often face trolling campaigns that can have serious consequences. In the Philippines, President Rodrigo Duterte's administration has faced allegations of employing a massive online army of trolls to manipulate public opinion. This army is accused of spreading propaganda, attacking political opponents, and silencing critics of policies like Duterte's war on drugs (Williams, 2021; Feldstein, 2021). Research has highlighted the coordinated nature of these trolling activities, impacting the digital rights of Filipinos by stifling free and open discourse (Bradshaw & Howard, 2017).

India has experienced a surge in political trolling across messaging applications and social media platforms. Political supporters and affiliated groups often orchestrate coordinated trolling campaigns to target opponents, journalists, and activists. This not only weakens constructive discourse but also fosters an environment where individuals fear expressing dissenting opinions on policies or cases of corruption, hindering the accountability of governments. Instances of political trolling are particularly noticeable during election seasons, where coordinated attacks on social media platforms seek to influence public opinion. In the lead-up to the 2023 local election in Karnataka State, disinformation and inflammatory content exploiting religious tensions between Hindus and Muslims were circulated via WhatsApp to advance the BJP's Hindu nationalist agenda and disparage political opponents. Quietly, the party has collaborated with campaign consultants and content creators to craft incendiary posts designed to go viral on WhatsApp (Shih, 2023).

During the 2014 prime ministerial campaign of Narendra Modi, there were allegations of coordinated social media trolling by India's ruling party, the Bharatiya Janata Party, targeting public figures. Former party troll Sadhavi Khosla claims that the trolling extended to religious and sexual dimensions, singling out political opponents like Rahul Gandhi and Bollywood star Aamir Khan (Safi, 2016).

In China, the government has been accused of deploying a significant number of online trolls to shape public opinion and stifle dissent. These trolls often engage in coordinated campaigns to flood social media platforms with nationalist sentiments, attacking individuals or entities perceived as critical of the Chinese government. The Chinese government's use of online trolls is a well-documented phenomenon (Harold et al, 2021), suggesting coordinated online campaigns during sensitive events, such as geopolitical tensions or incidents involving human rights issues.

Trolling is largely possible thanks to cybertroopers, individuals or groups employed to manipulate online information and influence public opinion. They often work in favour of political agendas, using various tactics to control narratives and sway public sentiment (Sastramidjaja & Wijayanto, 2022). During the 1Malaysia Development Berhad scandal in Malaysia, allegations surfaced of the deployment of cybertroopers to orchestrate online activities in support of the government. These cybertroopers were purportedly tasked with manipulating online discussions, steering narratives, and influencing public opinion to favour the ruling authorities. Research (Asia Centre, 2022b, 2023a) has delved into this phenomenon, uncovering a strategic use of social media platforms to disseminate misinformation, launch targeted attacks against those holding governments publicly accountable, and construct a digital environment that subverted the fundamental principles of free expression and transparency.

Cybertrooper activities have also been tracked in Pakistan. Fake social media profiles proliferated since the lead-up to the 2018 election, where it was found that the contesting cybertrooper groups vie for dominance over the digital information sphere. Their tactics have included spreading misleading or

false information, that in many cases serves to stir ill will against a minority group. For example, disinformation regarding politicians being "Jewish agents". Harassments have also targeted human rights defenders in the country, and such accounts were used to lure these individuals to share sensitive and personal information (such as passwords) or to install hacking tools (Bradshaw et al., 2021).

Hate Sites

Hate sites, platforms that disseminate discriminatory and harmful content targeting specific individuals or groups based on attributes such as race, religion, or ethnicity, pose a significant threat to civil society's ability to call out public policy lapses, corruption cases, and overstepping of authority, thus contributing to the spread of hate speech, discrimination, and violence (Asia Centre, 2023c).

Since the early 2010s, in Bangladesh, there have been deliberate online campaigns falsely accusing religious minorities of anti-Muslim blasphemy, leading to significant and fatal attacks on Hindus and Buddhists. One notable incident took place in 2012 when a photoshopped image of a burned Quran was circulated on a Buddhist youth's Facebook page (BBC, 2012). In retaliation, a mob, reportedly exceeding twenty thousand individuals, including political leaders from major parties, rampaged through the local Buddhist community in Cox's Bazar, Chattogram. This resulted in the destruction and looting of numerous homes and temples (Liebowitz et al., 2012).

The Rohingya – a stateless Muslim ethnic minority group primarily residing in Myanmar that faces persecution and displacement, often seeking refuge in neighbouring countries where they have been fighting for citizenship and equal treatment – crisis in Myanmar illustrates how online hate speech can result in offline consequences. This assertion is substantiated by specific evidence, particularly through the direct links established between online hate and offline violence. Facebook played a crucial role as a tool for the dissemination of anti-Rohingya hate speech, with instances where posts on the platform were directly responsible for inciting violence against the Rohingya Muslim community. These posts not only propagated hatred but also included explicit calls for acts such as killing and rape against the Rohingya population (Miles, 2018).

In South Korea, the proliferation of online communities spreading hate speech has notably targeted feminists to describe negative stereotypes about modern Korean women, seen as stereotypes of sophistication and Westernisation. For example, "bean paste girl" is a term used to describe a young, college-aged woman who saves money by eating affordable meals so she can spend extra money on things like Starbucks (Kim, 2021). Specific online platforms have emerged as breeding grounds for misogynistic content, cyberbullying, and doxxing campaigns aimed at individuals advocating for gender equality. A survey conducted by the National Human Rights Commission of Korea underscores the widespread impact, revealing that over 80% of South Koreans have encountered online hate speech, with women being the primary focus. The survey highlights the prevalence of hate speech against certain regions, feminists, and the elderly. In real-life scenarios, seniors, people from specific regions, and women emerge as the most frequently targeted groups. The majority of respondents perceive online hate speech as more severe than its real-life counterpart, pinpointing online news articles and comment sections as major sources of such content (Korea Times, 2021).

3e. Rise of Self-Inhibiting Behaviours Among INGOs and CSOs

In response to the pervasive content regulations and the prosecution of those seeking to hold governments accountable, civil society has adopted various strategies to safeguard themselves against the stringent regulation of the digital sphere in the region. This section provides an overview of five of these protective behaviours.

One practice some civil society actors adopt in response to governments' increased content monitoring is changing the topic of their work priority (Asia Centre, 2023d). Fundamental rights that are often perceived to be too political for public officials and government elites – such as freedom of expression, the right to peaceful assembly and association, and freedom of religion or belief – are de-prioritised and replaced by developmental issues or humanitarian assistance. Still, when CSOs work on the latter topics, they will avoid addressing structural issues or root causes of the problems that bring about challenges facing the communities (Fadnes, 2020). Doing so will question and disrupt the power dynamic empowerment of marginalised individuals or groups, or service delivery to affected communities (Asia Centre, 2022a).

Based on Asia Centre's cumulative experience, increasingly INGOs request their local CSO partners to remove their logos and mention support for activities and knowledge products. Instead, they prefer to hand over full discretion and responsibility to local partners without the past requisite of publicly acknowledging their organisation's support and insisting their logos are displayed on publicity materials. The practice now is to avoid any possible risk of being entangled in the government's rhetorical crossfires or legal action. Given this passing-the-buck scenario, local civil society actors sometimes practise the use of euphemisms in their activities and engagement with the public to avoid possible criminalisation from online content regulations, which impose lengthy jail terms or hefty fines on both individuals and organisations as well as being subjected to trolling and hate attacks.

It has also been observed that a growing number of individuals, as well as representatives from CSOs and INGOs, express a reluctance to appear in photos and videos captured during events like roundtables and workshops. The primary concern is to avoid being identified as participants. Additionally, many individuals and organisations choose not to report on the activities they organise. This reluctance extends to activities like refraining from posting on social media about events or being associated with activities organised by other organisations.

In terms of language use, opting for a minority language or English instead of the official languages in the relevant locality is also a strategy employed to position activities or knowledge products as outside the mainstream local context. These observed trends among INGOs and CSOs have been noted by the Asia Centre over the past few years.

There have also been alleged cases of technology firms changing the algorithm of their social media platforms to make politically sensitive content appear less frequently or reach fewer readers. In the case of Google, reports are showing that the company is changing how it displays disputed border areas in Google Maps depending on where the website is accessed – by displaying the look of the map that conforms with each government's views (Bensinger, 2020). Another side-effect of content regulations is that these legislations obligate technology companies to cooperate with the state or risk being forced out of the country. Self-censorship is then institutionalised by technology companies. In 2020, Facebook, for example, banned an account of Vietnamese activist Bui Van Thuan permanently after a

land dispute between local villagers and the government erupted (Cloud & Bengali, 2020). The action was claimed to be a direct request from the government.

The examples provided above, along with the cases discussed in previous sections of this chapter, highlight the significant impact of the increasing number of online regulations enforced through legal provisions on civil society in the Asia-Pacific region. These regulations have weakened civil society's capacity to hold governments accountable for their public policies. The repercussions range from the overcriminalisation of individuals seeking greater public accountability to the emergence of new behaviours in response to these regulations. In essence, online content regulations are taking a toll on civil society in the region. The subsequent chapter will present a set of policy recommendations aimed at enhancing civil society's ability to hold governments accountable, irrespective of the challenges posed by these restrictions.

4. Recommendations

The popularity of the internet, social media platforms, and messaging applications has resulted in a wide range of opportunities for civil society to keep political officeholders and government officials accountable for their actions. In response, governments introduced a suite of legal measures, which has weakened civil society's ability to hold governments accountable for actions and as well as lapses in their public policies. The final chapter of this report presents a set of policy recommendations for a range of actors to ensure that civil society's capacity to hold the government accountable in the digital age is not negated but, instead, enhanced.

International Organisations

- The UN should advocate for member states to prioritise the implementation of recommendations stemming from the Universal Periodic Review (UPR) process and those put forth by Special Rapporteurs. Specifically, the focus should be on amending or repealing restrictive laws that have a detrimental impact on the ability of civil society to hold governments accountable.
- The UN should give precedence to Sustainable Development Goal (SDG) 16.10 (ensure public access to information and protect fundamental freedoms) when engaging with member states for civil society to have the appropriate access to information to hold governments accountable for their public policies.
- The UN and INGOs should enhance their financial support and establish dedicated budget allocations to provide technical assistance for the online initiatives of civil society. This support should aim to fortify the online safety of civil society actors by enabling them to leverage digital security tools and adhere to best practices in digital hygiene.

Governments

- Sign and ratify international human rights treaties, such as the International Covenant on Civil and Political Rights, which safeguard freedom of expression, including the freedom to criticise public policies and government officials. Additionally, they should ensure diligence in fulfilling reporting obligations to the treaty bodies.
- Amend and repeal vaguely-worded provisions within electronic and computer usage laws in order to prevent the unwarranted criminalisation of civil society actors.
- Avoid inducing a chilling effect and fostering a climate of self-censorship by refraining from employing vague online content regulations against human rights defenders and civil society organisations.
- Enact and enforce comprehensive privacy laws, particularly for those who have not yet done so, requiring technology companies to proactively address the challenge posed by online trolls and similar entities.

Internet Service Providers and Technology Companies

- Refuse government notice-and-take-down orders, especially if compliance results in negating calls for government accountability of public policies.
- Consistently publicise comprehensive transparency reports that detail government requests for removal and blocking, as well as instances of state-supported information operations, ensuring continued openness and accountability.
- Conduct a comprehensive review of community standards to prioritise the amplification of civil society voices that call out lapsus in public policies, while refusing to block or remove accounts of individuals and organisations that call for government accountability.
- Take proactive measures to combat disinformation, especially against civil society, on platforms by flagging false and hateful content, and clearly labelling content originating from state-controlled media.
- Promote and actively support digital media literacy, collaborating with civil society, governments, media organisations, and international entities to promote public accountability.
- In instances where these measures are not currently implemented, institute robust policies requiring the disclosure of sources contributing to trolling and defamation.

Civil Society Actors

INGOs

- Contribute input to international standards and actively engage with governments during the promulgation of new laws to ensure that fair criticism of public policies and that of political office holders and government officials are not made illegal.
- Provide support to local CSOs, human rights defenders, and other members of civil society by conducting risk assessments and delivering comprehensive digital security training.

CSOs

- Build inclusive local coalitions to advocate for government accountability of public policy and access to information. Engage directly with lawmakers to emphasise the importance of these issues.
- Enhance public awareness regarding online content regulations and their repercussions, including actively monitoring and documenting instances of harassment and prosecutions of those who advocate for public accountability.

Independent Media

- Maintain independence from government influence by upholding rigorous standards of journalistic quality that emphasise government accountability that is accepted and trusted by the public.
- Promote transparency on editorial independence by implementing pre-publication fact-checks on content to ensure that reports on government public policy lapses are not politically countered as fake news.

5. Conclusion

With increased internet penetration and the popularity of social media and messaging applications, these digital tools have transformed how individuals and organisations interact, communicate and mobilise to advocate for social and political causes. Civil society in the Asia-Pacific region has found in digital media a new platform to amplify its voice and keep political officeholders, government officials and policies publicly accountable.

However, governments in the region have tightened up their grip over the digital sphere to mitigate the political ill-effects of being called out on policy lapses. Fearing the risk of delegitimisation, governments are resorting to justifications of tackling disinformation, hate speech, and defamation to enact new legislation and leverage outdated laws - like penal codes and national security laws - to curate their preferred hegemonic narratives. These strategies have targeted individuals, CSOs, internet service providers, and technology companies, aiming to censor and inflict reputation damage on all those who call for public government accountability.

Actions include the removal of online content, disruptions to internet services, fines, and imprisonment for civil society members. In recent years, a notable shift has been observed, transitioning from the use of laws to indirectly facilitating trolling by cybertroopers and allowing the proliferation of hate sites as the new unspoken strategy that neutralises and casts aspersions on those who call for government accountability.

The weakening of civil society's ability to hold governments publicly accountable in the digital sphere is evident as INGOs and CSOs strive to avoid legal prosecution and hate attacks. As a result, INGOs, seeking discretion, chose to remain in the background and operate through local sub-grantees, while CSOs are scaling back their public communication, often resorting to English or non-majority languages to navigate state censorship in their advocacy efforts. ISPs and technology companies, aiming to avoid liability, may strike deals with governments to filter out criticism in exchange for continued operations.

In the Asia-Pacific region, where elections often fall short of driving meaningful policy changes and corruption remains a pervasive issue, the importance of public accountability is underscored. Here, civil society's independence becomes crucial in bridging the gap between electoral mandates and effective governance. Independent CSOs act as vital checks on power, advocating for diverse citizen interests, and providing objective scrutiny. In a context where traditional democratic processes face challenges, an independent civil society emerges as the linchpin for fostering genuine accountability and responsive governance.

To push back, a multi-stakeholder and coordinated approach involving both state and non-state actors is essential to ensure that civil society can exercise its fundamental right to call out governmental lapses in public policy. Only through collective efforts, can content regulations not become a restraint on civil society’s right to keep government officials and policies publicly accountable.

Bibliography

AccessNow (2023) 'Resist Myanmar's digital coup: stop the military consolidating digital control', AccessNow, at: https://www.accessnow.org/press-release/myanmars-digital-coup-statement.

AccessNow (2023a) 'Indonesians seek justice after internet shutdown', AccessNow, at: https://www.accessnow.org/indonesians-seek-justice-after-internet-shutdown.

AccessNow (2023b) 'Who is shutting down the internet in 2023? A mid-year update', AccessNow, at: https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update.

Ailawadi, Aayush (2018) 'India, the world's largest democracy, blocks more websites than Pakistan', NDTV, at: https://www.ndtvprofit.com/technology/2018/04/26/india-the-worlds-biggest-democracy-blocks-more-websites-than-pakistan.

Amin, Tahir (2021) 'Procedure, oversight and safeguards "Removal & Blocking of Unlawful Online Content Rules, 2021" modified', Business Recorder, at: https://www.brecorder.com/news/40101984.

Angara, Edgardo J. (2012) 'Explanatory Note', Philippines Senate, at: http://legacy.senate.gov.ph/lisdata/1427912043!.pdf.

Angwalkar, Shreetesh (2021) 'Sri Lanka implements Singapore style law to control fake news', Spherex, at: https://www.spherex.com/regulation/sri-lanka-implements-singapore-style-law-to-control-fake-news.

Arshad Khan, Eesha (2016) 'The Prevention of Electronic Crimes Act 2016: An analysis', at: https://sahsol.lums.edu.pk/node/12862.

Article19 (2021) 'Indonesia: Regulation of the Minister of Communication and Informatics Number 5 of 2020 on Private Electronic System Operators (Ministerial Regulation 5)', Article19, at: https://www.article19.org/wp-content/uploads/2021/09/Legal-Analysis-Indonesia-Ministerial-Regulation-5.pdf.

ASEAN Youth Forum (nd.) 'SEAYOUTH 2022', ASEAN Youth Forum, at: https://festival.aseanyouthforum.org.

Asia Centre (2020) *Hate Speech in Southeast Asia: New Forms, Old Rules*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/2020/07/Hate-Speech-in-Southeast-Asia-New-Forms-Old-Rules.pdf.

Asia Centre (2021a) *Internet Freedoms in Cambodia: A Gateway to Control*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Internet-Freedoms-in-Cambodia-A-Gateway-to-Control.pdf.

Asia Centre (2021b) *Harmony Laws in Southeast Asia: Majority Dominance, Minority Repression*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Harmony-Laws-in-Southeast-Asia-Majority-Dominance-Minority-Repression.pdf.

Asia Centre (2022a) *Foreign Interference Laws in Southeast Asia: Deepening the Shrinkage of Civic Space*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Foreign-Interference-Laws-in-Southeast-Asia-Deepening-the-Shrinkage-of-Civic-Space.pdf.

Asia Centre (2022b) *Youth and Disinformation in Malaysia: Strengthening Electoral Integrity*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Youth-and-Disinformation-in-Malaysia-Strengthening-Electoral-Integrity-1.pdf.

Asia Centre (2023a) *Internet Freedoms in Malaysia: Regulating Online Discourse on Race, Religion and Royalty*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Internet-Freedoms-In-Malaysia-Regulating-Online-Discourse-on-Race-Religion-and-Royalty-.pdf.

Asia Centre (2023b) *State-Sponsored Online Disinformation: Impact on Electoral Integrity in Thailand*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/State-Sponsored-Online-Disinformation-Impact-on-Electoral-Integrity-in-Thailand.pdf.

Asia Centre (2023c) *Political Hate Sites in Singapore: Flourishing Without Repercussions*, Bangkok: Asia Centre, at: https://asiacentre.org/wp-content/uploads/Political-Hate-Sites-in-Singapore-Flourishing-Without-Repercussions.pdf.

Asia Centre (2023d) 'Restrictive Laws Spur Self-censorship and Euphemisms in Journalism', Asia Centre, at: https://asiacentre.org/restrictive-laws-spurr-self-censorship-and-euphemisms-in-journalism.

BBC (2012) 'Bangladesh rampage over Facebook Koran image', BBC, at: https://www.bbc.com/news/world-asia-19780692.

BBC Thai (2023) 'ศาลอนุญาตประกันตัว ไอซ์-รักชนก รอดนอนคุก หลังศาลตัดสินจำคุก 6 ปี คดี ม.112 และ พ.ร.บ.คอมฯ *[The court granted bail to Ice-Rakchanok after the court sentenced her to 6 years in prison in the Section 112 and Computer Act case]*', BBC Thai, at: https://www.bbc.com/thai/articles/cgr38q36erro.

Bensinger, Greg (2020) 'Google redraws the borders on maps depending on who's looking', Washington Post, at: https://www.washingtonpost.com/technology/2020/02/14/google-maps-political-borders.

Bhat, Mehran and Rina Chandran (2022) 'FEATURE-'Living in the stone age': Offline for 18 months in Indian Kashmir', Reuters, at: https://www.reuters.com/article/idUSL8N2YZ245.

Biyani, Neeti, Noelle Francesca De Guzman, Namrata Maheshwari and Shahzeb Mahmood (2021) 'Internet Impact Brief: Bangladesh: Regulation for Digital, Social Media and OTT Platforms, 2021', Internet Society, at: https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-bangladesh-regulation-for-digital-social-media-and-ott-platforms-2021.

Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard (2020) *Industrialised Disinformation: 2020 Global Inventory of Organised Social Media Manipulation*, Computational Propaganda Research Project, Oxford Internet Institute, at: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf.

Chew, Wei Chun (2018) 'How it works: Great Firewall of China', Medium, at: https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475.

China Index (2022) 'Countries and Territories', China Index 2022, at: https://china-index.io/country.

CISOMAG (2020) 'Singapore blocks Malaysian website under falsehoods law', CISOMAG, at: https://cisomag.com/singapore-blocks-malaysian-website-lawyers-for-liberty.

CIVICUS (2022) 'Malaysian police continue to harass protesters and activists and criminalise online expression', CIVICUS, at: https://monitor.civicus.org/explore/malaysian-police-continue-harass-protesters-and-activists-and-criminalise-online-expression.

Cloud, David S. and Shashank Bengali (2020) 'Facebook touts free speech. In Vietnam, it's aiding in censorship', LA Times, at: https://www.latimes.com/world-nation/story/2020-10-22/facebook-censorship-suppress-dissent-vietnam.

CNA (2023) 'POFMA restrictions imposed on Kenneth Jeyaretnam's website, social media pages over "multiple falsehoods"', CNA, at: https://www.channelnewsasia.com/singapore/pofma-kenneth-jeyaretnam-website-social-media-falsehoods-dol-3980166.

Department of Information Services (2019) 'Cabinet passes draft amendments to three laws to combat fake news', Executive Yuan (Taiwan), at: https://english.ey.gov.tw/Page/61BF20C3E89B856/54da6086-c403-4e5b-a549-8101759993df

Dien Nguyen An Luong (2022) 'No News is Good News: Low Trust in Southeast Asia's Mainstream Media', Fulcrum, at: https://fulcrum.sg/no-news-is-good-news-low-trust-in-southeast-asias-mainstream-media.

OHCHR, 'Digital Security Act', OHCHR, at: https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf.

Economy, Elizabeth C. (2018) 'The great firewall of China: Xi Jinping's internet shutdown', The Guardian, at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

EU (2021) 'Vietnam: Statement by the Spokesperson on the sentencing of three journalists', EU, at: https://www.eeas.europa.eu/eeas/vietnam-statement-spokesperson-sentencing-three-journalists_en.

Fadnes, Ingrid, Roy Krøvel and Anna Grøndahl Larsen (2020) *Journalist Safety and Self-Censorship*, London: Routledge, at: DOI:10.4324/9780367810139.

Feldstein, Steven (2021) 'Social Manipulation and Disinformation in the Philippines', in *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, Oxford, Oxford University Press, at: https://academic.oup.com/book/39418.

Free Malaysia Today (2023) 'MACC chief's libel suit against journalist to be heard in July next year', Free Malaysia Today, at: https://www.freemalaysiatoday.com/category/nation/2023/03/13/macc-chiefs-libel-suit-against-journalist-to-be-heard-in-july-next-year.

Ghonim, Wael (2012) *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir*, Boston, MA: Houghton Mifflin Harcourt.

Global Network Initiative (2023) 'GNI Analysis: Information Technology Rules Put Rights at Risk in India', Global Network Initiative, at: https://globalnetworkinitiative.org/india-it-rules-2021.

Goel, Vindu, Hari Kumar and Sheera Frenkel (2018) 'In Sri Lanka, Facebook contends with shutdown after mob violence', New York Times, at: https://www.nytimes.com/2018/03/08/technology/sri-lanka-facebook-shutdown.html.

Gomez, James and Yawee Butrkrawee (2022) 'Political Criticism as Fake News: How Brunei, Laos and Vietnam Suppress Democracy', in *Fake News and Elections in Southeast Asia Impact on Democracy and Human Rights*, edited by James Gomez and Robin Ramcharan, London: Routledge.

Google (2023) 'Government requests to remove content', Google, at: https://transparencyreport.google.com/government-removals/overview.

Gunatilleke, Gehan (2016) 'Hate speech in Sri Lanka: How a new ban could perpetuate impunity', Oxford Human Rights Hub, at: https://ohrh.law.ox.ac.uk/hate-speech-in-sri-lanka-how-a-new-ban-could-perpetuate-impunity

Hale, Erin (2023) 'US says China can spy with TikTok. It spies on world with Google', Aljazeera, at: https://www.aljazeera.com/economy/2023/3/28/bid-to-ban-tiktok-raises-hypocrisy-charge-amid-global-spying.

Harold, Scott W., Nathan Beauchamp-Mustafaga and Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media*, Santa Monica, CA: RAND, at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z3/RAND_RR4373z3.pdf.

Hul Reaksmey (2020) 'Cambodia must end legal attacks on media, rights groups say', VOA News, at: https://www.voanews.com/a/press-freedom_cambodia-must-end-legal-attacks-media-rights-groups-say/6198012.html.

IFJ (2020) 'India: A grim milestone, 365 days of internet shutdown in Kashmir', IFJ, at: https://www.ifj.org/media-centre/news/detail/category/press-releases/article/india-a-grim-milestone-365-days-of-internet-shutdown-in-kashmir.

Janjua, Haroon (2022) 'Pakistan moves to stifle social media dissent', DW, at: https://www.dw.com/en/pakistan-new-cybercrime-law-threatens-to-to-stifle-social-media-dissent/a-60899561.

Janti, Nur (2023) 'Luhut's defamation trial against activists kicks off', Jakarta Post, at: at: https://www.thejakartapost.com/indonesia/2023/04/03/luhuts-defamation-trial-against-activists-kicks-off.html.

Januya, Andrea and Funakoshi Minami (2021) 'Myanmar's internet suppression', Reuters, at: https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo.

Kao, Kimberly (2023) 'China's Tencent wants to expand its presence in Singapore – and Chinese tourists are a big reason', CNBC, at: https://www.cnbc.com/2023/02/03/tencents-weixin-sees-singapore-as-a-strategic-market.html

Kathmandu Post (2024) 'Cabinet passes rules to regulate social media', Kathmandu Post, at: https://kathmandupost.com/national/2023/11/10/cabinet-passes-rules-to-regulate-social-media

Kemp, Simon (2014) 'Digital 2014: Global Digital Overview', Datareportal, at: https://datareportal.com/reports/digital-2014-global-digital-overview.

Kemp, Simon (2023a) 'Digital 2023: Global Overview Report', Datareportal, at: https://datareportal.com/reports/digital-2023-global-overview-report.

Kemp, Simon (2023b) 'Post Tagged Southeastern Asia', Datareportal, at: https://datareportal.com/reports/?tag=Southeastern+Asia.

Kemp, Simon (2023c) 'Post Tagged Eastern Asia', Datareportal, at: https://datareportal.com/reports/?tag=Eastern+Asia.

Kemp, Simon (2023c) 'Post Tagged Southern Asia', Datareportal, at: https://datareportal.com/reports/?tag=Southern+Asia.

Kim, Jack (2016) 'Thousands protest in South Korea, demand president quit over scandal', Reuters, at: https://www.reuters.com/article/us-southkorea-politics-idUSKCN12T08V.

Kim, Youngmi (2021) 'Mirroring Misogyny in Hell Choson: Megalia, Womad, and Korea's Feminism in the Age of Digital Populism', European Journal of Korean Studies 20(2): 101–133, DOI:10.33526/EJKS.20212002.101.

Kimseng, Meng (2014) 'Shaping Political Change: The Role of Social Media in Cambodia's 2013 Elections', *Asia Pacific Media Educator* 24(1): 107–116, at: DOI:10.1177/1326365X14539201.

Kobayashi, Yugo (2022) 'Stand Your Ground Against Anonymous Online Harassers With Amended Provider Liability Limitation Act', Chuo Sogo Law Office, at: https://www.clo.jp/english/wp-content/uploads/2023/02/Lexology_Article_CLO_Dec2022_E.pdf.

Koetsier, John (2023) '10 Most Downloaded Apps Of 2022: Facebook Down, Spotify Up, TikTok Stable, CapCut Keeps Growing', Forbes, at: https://www.forbes.com/sites/johnkoetsier/2023/01/04/top-10-most-downloaded-apps-of-2022-facebook-down-spotify-up-tiktok-stable-capcut-keeps-growing.

Korea Times (2023) 'Women are most frequent target of online hate speech in Korea: survey', Korea Times, at: https://www.koreatimes.co.kr/www/nation/2023/12/113_315038.html.

Kulshreshth, Shantanu (2023) '"Social Media Is the Second Ambedkar": Bhim Army and Social Media Mobilisation in North India, South Asia: *Journal of South Asian Studies*, DOI: 10.1080/00856401.2023.2216514.

Kurohi, Rei (2021) 'The Online Citizen taken offline, ahead of deadline set by IMDA after failure to declare funding', The Straits Times, at: https://www.straitstimes.com/singapore/the-online-citizen-goes-dark-ahead-of-deadline-set-by-imda.

Kyaw Hsan Hlaing (2020) 'People in parts of myanmar are living under the world's longest internet shutdown. It's putting lives in danger', Time, at: https://time.com/5910040/myanmar-internet-ban-rakhine.

Liebowitz, Jeremy, Geoffrey Macdonald, Vivek Shivaram, and Sanjendra Vignaraja (2021) 'The Digitalization of Hate Speech in South and Southeast Asia: Conflict-Mitigation Approaches', Georgetown Journal of International Affairs, at: https://gjia.georgetown.edu/2021/05/05/the-digitalization-of-hate-speech-in-south-and-southeast-asia-conflict-mitigation-approaches.

LiveLaw (2023) 'Laws needed to address fake news & hate speech in social media: Supreme Court judge Justice S Ravindra Bhat', LiveLaw, at: https://www.livelaw.in/top-stories/laws-needed-to-address-fake-news-hate-speech-in-social-media-justice-s-ravindra-bhat-223197.

Meta (2023) 'Content restrictions based on local law', Meta, at: https://transparency.fb.com/reports/content-restrictions.

Miles, Tom (2018) 'U.N. investigators cite Facebook role in Myanmar crisis', Reuters, at: https://www.reuters.com/article/idUSKCN1GO2Q4.

Myanmar Now (2022) 'Myanmar junta court sentences Japanese filmmaker to 7 years in prison', Myanmar Now, at: https://myanmar-now.org/en/news/myanmar-junta-court-sentences-japanese-filmmaker-to-7-years-in-prison.

Nreage BD (2022) ' Internet services disrupted in Barishal amid BNP's divisional rally', Newage BD, at: https://www.newagebd.net/article/185580/internet-services-disrupted-in-barishal-amid-bnps-divisional-rally.

Newage BD (2024) 'Internet shutdown weaponised against opposition, says BNP', Newage, at: https://www.newagebd.net/article/207649/internet-shutdown-weaponised-against-opposition-says-bnp.

Noeurn Davin and Lors Liblib (2023) 'Cambodian Government Blocks News sites before unopposed election', VOA, at: https://www.voanews.com/a/cambodian-government-blocks-news-sites-before-unopposed-election-/7185151.html.

OHCHR (2022) 'OHCHR Technical Note to the Government of Bangladesh on review of the

Perrigo, Billy (2020) 'The inside story of how Signal became the private messaging app for an age of fear and distrust', Time, at: https://time.com/5893114/signal-app-privacy.

Piga, Ashlee (2022) 'The rise of user-generated content And its impact on brand loyalty and affinity', Forbes, at: https://www.forbes.com/sites/forbesagencycouncil/2022/09/12/the-rise-of-user-generated-content-and-its-impact-on-brand-loyalty-and-affinity.

Priya, Anu (nd.) 'Terrorism in South Asia', Mahatma Gandhi Central University, at: https://mgcub.ac.in/pdf/material/20200417103529842651e27b.pdf.

Ratcliffe, Rebecca (2023) 'Dictator Hun Sen shuts down Cambodia's VOD broadcaster', The Guardian, at: https://www.theguardian.com/world/2023/feb/13/dictator-hun-sen-shuts-down-cambodias-vod-broadcaster.

Reuters (2015) 'Thailand scraps unpopular Internet "Great Firewall" plan', Reuters, at: https://www.reuters.com/article/us-thailand-internet-idUSKCN0S916I20151015.

Reuters Institute (2023) *Digital News Report*, Reuters Institute, at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf.

RFA (2021) 'Vietnamese Facebook user fined for 'Fake News' as criticism grows of government's handling of pandemic', RFA, at: https://www.rfa.org/english/news/vietnam/fine-09032021182640.html.

RFA Burmese (2021) 'Myanmar junta bans Irrawaddy news agency after months of harassment', RFA, at: https://www.rfa.org/english/news/myanmar/irrawaddy-10312022181138.html.

Rowe, Jacqueline & Saba Mah'derom (2023) 'Weaponizing internet shutdowns to evade accountability for rights violations', Open Global Rights, at: https://www.openglobalrights.org/weaponizing-internet-shutdowns-evade-accountability-rights-violations.

RSF (2021) 'Five media outlets shut down in Myanmar, one raided', RSF, at: https://rsf.org/en/five-media-outlets-shut-down-myanmar-one-raided.

RSF (2023) 'Singapore authorities must lift arbitrary edict blocking Asia Sentinel website', RSF, at: https://rsf.org/en/singapore-authorities-must-lift-arbitrary-edict-blocking-asia-sentinel-website.

Safi, Michael (2016) 'India's ruling party ordered online abuse of opponents, claims book', The Guardian, at: https://www.theguardian.com/world/2016/dec/27/india-bjp-party-ordering-online-abuse-opponents-actors-modi-claims-book.

Sang-Hun, Choe (2021) 'South Korea Shelves "Fake News" Bill Amid International Outcry', New York Times, at: https://www.nytimes.com/2021/10/01/world/asia/south-korea-fake-news-law.html.

Sastramidjaja, Yatun and Wijayanto (2022) *Cyber Troops, Online Manipulation of Public Opinion and Co-Optation of Indonesia's Cyberspher*, Singapore: ISEAS, at: https://www.iseas.edu.sg/wp-content/uploads/2022/03/TRS7_22.pdf.

Shewale, Rohit (2023) '18+ WeChat Statistics For 2024 (Users, Revenue & More)', Demandsage, at: https://www.demandsage.com/wechat-statistics.

Singapore Police Force (2020) 'Youth arrested for inciting violence and posting religious hate comments on social media', Singapore Police Force, at: https://www.police.gov.sg/media-room/news/20200609_arrest_j_youth_arrested_for_inciting_violence_and_posting_religious.

Social Media Victims Law Center (2023) 'What is trolling on social media?', Social Media Victims Law Center, at: https://socialmediavictims.org/cyberbullying/types/trolling.

Tech Wire Asia (2010) 'Southeast Asia dominates Facebook's fastest growing list', Tech Wire Asia, at: https://techwireasia.com/07/2010/southeast-asia-dominates-facebooks-fastest-growing-list.

Telling, Oliver & Criddle, Cristina (2022) 'Big Tech signs up to Indonesia's strict content law', Financial Times, at: https://www.ft.com/content/6f9eebf5-6025-44b6-8815-9e0ee4096726.

The Business Times (2023) 'Meta, TikTok report jump in Malaysia government requests to remove content in 2023', The Business Times, at: https://www.businesstimes.com.sg/international/asean/meta-tiktok-report-jump-malaysia-government-requests-remove-content-2023.

The Business Standard (2022) 'Mobile internet service slowed down in Khulna amid BNP rally', The Business Standard, at: https://www.tbsnews.net/bangladesh/mobile-internet-service-slowed-down-khulna-amid-bnp-rally-518282.

The Jakarta Post (2019) '#ReformCorrupted', The Jakarta Post, at: https://www.thejakartapost.com/academia/2019/09/25/reformcorrupted-1569384427.html.

TLHR (2023) 'พฤศจิกายน 2566: จำนวนผู้ถูกดำเนินคดีทางการเมืองยอดรวม 1,935 คน ใน 1,262 คดี [*November 2023: The total number of people facing political prosecutions is 1,935 in 1,262 cases*]', TLHR, at: https://tlhr2014.com/archives/61998.

TrailWatch (2023) 'Section 20 of Pakistan's Prevention of Electronic Crimes Act: Urgent Reforms Needed', Clooney Foundation for Justice, at: https://cfj.org/wp-content/uploads/2023/10/Pakistan_PECA-Report_September-2023.pdf.

USAID (2014) 'Social Networking: A Guide to Strengthening Civil Society Through Social Media', USAID, at: https://pdf.usaid.gov/pdf_docs/pa00jx4x.pdf.

Williams, Sean (2017) 'Rodrigo Duterte's army of online trolls', New Republic, at: https://newrepublic.com/article/138952/rodrigo-dutertes-army-online-trolls.

Wong, Andy Ming Jun (2023) 'Singapore censors ANU's East Asia Forum website', Pearls and Irritations, at: https://johnmenadue.com/singapore-censors-anus-east-asia-forum-website.

"Amendments to IT Rules" (2021), Parliamentary Research Service India, at: https://prsindia.org/billtrack/amendments-to-it-rules-2021.

"Anti-Fake News Bill" (2018), CLJ Law, at: https://www.cljlaw.com/files/bills/pdf/2018/MY_FS_BIL_2018_06.pdf.

"Bangladesh Telecommunications Act" (2001), International Telecommunication Union, at: https://www.itu.int/ITU-D/treg/Documentation/Bangladesh/BTRC-TelecomLaw2001.pdf.

"Broadcasting Act" (1994), Singapore Statutes Online, Attorney-General's Chambers of Singapore, at: https://sso.agc.gov.sg/Act/BA1994?ProvIds=P1IX-.

"Communications and Multimedia Act" (1998), Malaysian Communications and Multimedia Commission, at: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Act588bi_3.pdf.

"Computer-related Crime Act" (2007), iLaw, at: https://freedom.ilaw.or.th/sites/default/files/CCA_EN.pdf.

"Criminal Code (Cambodia)" (2001), Asian Judges Network on Environment, at: https://www.ajne.org/sites/default/files/resource/laws/7195/criminal-code-cambodia-en-kh.pdf.

"Cybercrime Prevention Act" (2012), Philippines Official Gazette, at: https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175.

"Cybersecurity Law" (2022) (Draft), EngageMedia, at: https://engagemedia.org/wp-content/uploads/2022/02/2022-MM-Cybersecurity-Law-ENG.pdf.

"Decree No. 53/2022/ND-CP" (2022), Law Net, at: https://lawnet.vn/en/vb/Decree-53-2022-ND-CP-elaborating-the-Law-on-cybersecurity-of-Vietnam-80D86.html.

"Digital Security Act" (2018), Bangladesh Association of Software & Information Services, at: https://basis.org.bd/public/files/policy/5e1653db166e8Digital-Security-Act-2018-English-version.pdf.

"Electronic Transactions Law" (2004), Myanmar Trade Portal, at: https://www.myanmartradeportal.gov.mm/uploads/legals/2018/12/Electronic%20Transactions%20Law%202004(English).pdf.

"Electronic Transactions Law" (2021), Myanmar Centre for Responsible Business, at: https://www.myanmar-responsiblebusiness.org/pdf/electronic-transactions-law_consolidated_2014-and-2021_en.pdf.

"Indian Penal Code" (1860), India Code, at: https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362.

"Pakistan Telecommunication (Re-organization) Act" (1996), Pakistan Telecommunication Authority, at: https://www.pta.gov.pk/en/laws-&-policies/act.

"Penal Code (Thailand)" (1956), Thailand Law Online, at: https://www.thailandlawonline.com/table-of-contents/criminal-law-translation-thailand-penal-code.

"Prevention of Electronic Crime Act" (2016), National Assembly of Pakistan, at: https://na.gov.pk/uploads/documents/1470910659_707.pdf.

"Prohibition of Fake News on Social Media Bill" (2023), Parliament of India, at: https://sansad.in/getFile/BillsTexts/LSBillTexts/Asintroduced/47%20OF%202023%20AS%20INTRO84202372634PM.pdf?source=legislation.

"Protection from Online Falsehoods and Manipulation Act" (2019), Singapore Statutes Online, Attorney-General's Chambers of Singapore, at: https://sso.agc.gov.sg/Act/POFMA2019.

"Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules" (2021), Ministry of Information, Technology and Telecommunication, at: https://moitt.gov.pk/SiteImage/Misc/files/Removal%20Blocking%20of%20Unlawful%20Online%20Content%20Rules%202021.PDF.

"Sub-decree No. 23 on the establishment of National Internet Gateway (NIG)" (2021), Open Development Cambodia, at: https://data.opendevelopmentcambodia.net/laws_record/sub-decree-no-23-on-the-establishment-of-national-internet-gateway-nig.

"Telecommunications Law" (2015), Myanmar Law Information System, at: https://www.mlis.gov.mm/mLsView.do;jsessionid=873EF072104248EAB3CBDDB2DE19F143?lawordSn=1076.

"Temporary Suspension of Telecom Services (Public Emergency or Public Safety)" Rules (2017), Department of Telecommunications, at: https://dot.gov.in/circulars/temporary-suspension-telecom-services-public-emergency-or-public-safety-rules-2017.

"Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik *[Law of the Republic of Indonesia No. 11 of 2008 about Information And Electronic*

Transactions]" (2008), National Assembly of Indonesia, at: https://www.dpr.go.id/doksetjen/dokumen/-Regulasi-UU.-No.-11-Tahun-2008-Tentang-Informasi-dan-Transaksi-Elektronik-1552380483.pdf.

"Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik *[Laws of the Republic of Indonesia No. 19 of 2016 about Amendments to the Law No. 11 of 2008 about Information And Electronic Transactions]*" (2016), Ministry of Communications and Information, at: https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf.

"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) *[Computer-Related Crime Act (No.2)]*", Thailand Official Gazette, at: https://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF.

ASIACENTRE

Asia Centre is a civil society research institute with Special Consultative Status with the United Nations Economic and Social Council (UN ECOSOC). The Centre's core activities involve research, capacity-building, advocacy, and media initiatives, focusing on four key themes: freedom of religion or belief, freedom of speech, freedom of association, and the right to political participation. Asia Centre collaborates with civil society stakeholders, international non-governmental organisations (INGOs), and parliamentarians to support their respective initiatives. It operates from offices in Bangkok (Thailand), Johor Bahru (Malaysia), and Phnom Penh (Cambodia).

Asia Centre
Asia Centre
Asia Centre
@asiacentre_org
asiacentre_org
asiacentre

website: asiacentre.org
email: contact@asiacentre.org