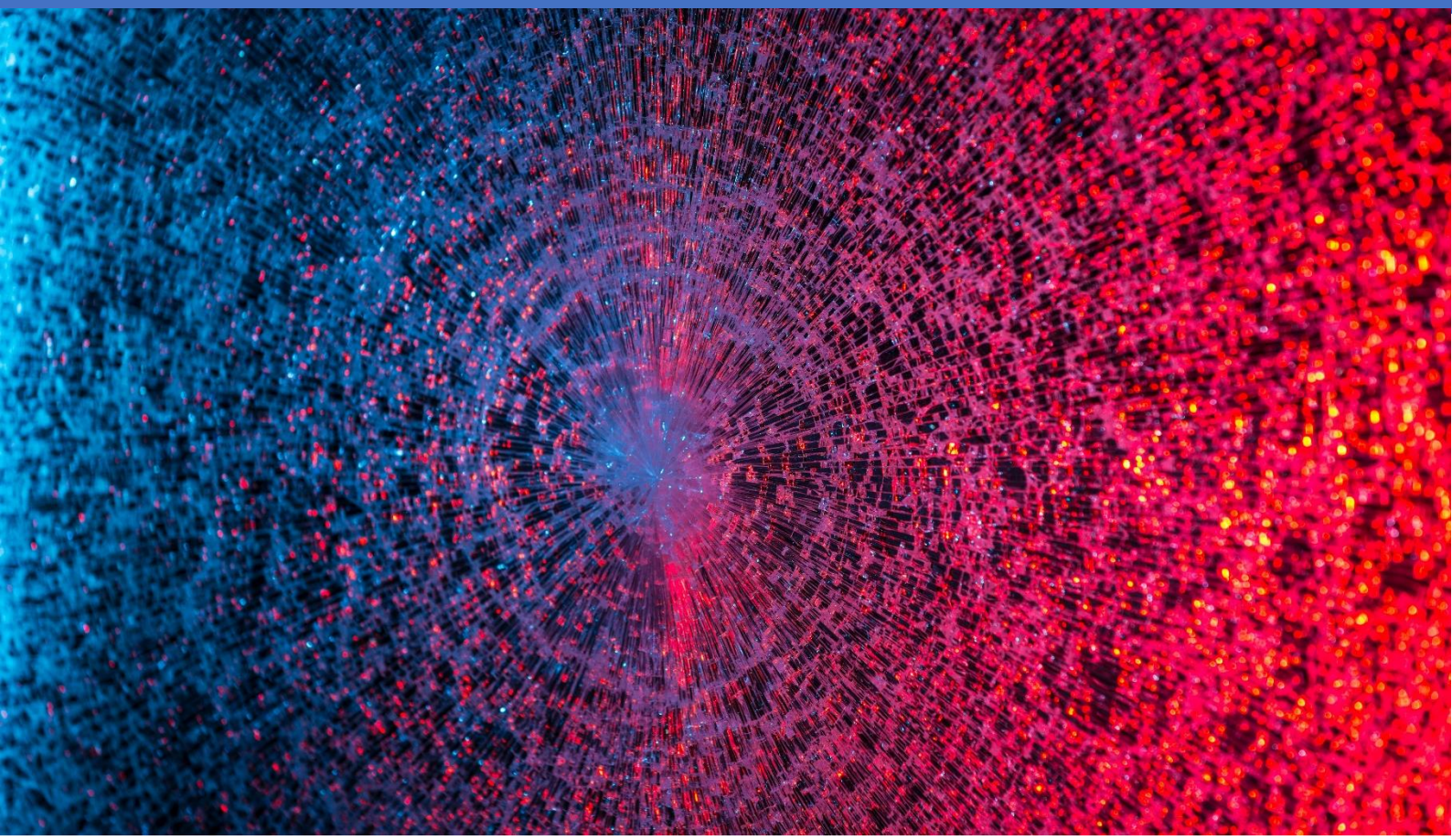
Internet Freedoms in Thailand

August 2022



ASIACENTRE

DESTINATION JUSTICE

Copyright © 2022 Asia Centre. All rights reserved.

Permission Statement: No part of this report in printed or electronic form may be reproduced, transmitted or utilised in any form or by any means, electronic, mechanical, photocopying or otherwise, without written permission of the Asia Centre.

Copyright belongs to Asia Centre unless otherwise stated.

Civil society organisations and educational institutions may use this report without requesting permission on the strict condition that such use is not for commercial purposes.

When using or quoting this report, every reasonable attempt must be made to identify owners of the copyright.

Errors or omissions will be corrected in subsequent editions.

Requests for permission should include the following information:

- The title of the document for which permission to copy material is desired.
- A description of the material for which permission to copy is desired.
- The purpose for which the copied material will be used and the manner in which it will be used.
- Your name, title, company or organisation name, telephone number, e-mail address and mailing address.

Please send all requests for permission to:

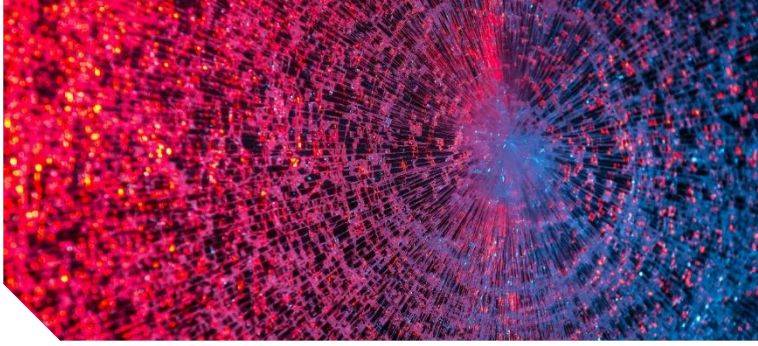
Asia Centre
128/183 Phayathai Plaza Building (17th Floor),
Phayathai Road, Thung-Phayathai,
Rachatewi, Bangkok 10400 Thailand
info@asiacentre.org

Table of Contents

Abbreviations

AHRC	Asian Human Rights Commission
AHRD	ASEAN Human Rights Declaration
AICHR	ASEAN Intergovernmental Commission on Human Rights
AMRI	ASEAN Ministers Responsible for Information
ANNI	Asian NGO Network on National Human Rights Institutions
AOT	Airports of Thailand
ASEAN	Association of Southeast Asian Nations
CAT	Communications Authority of Thailand
CCA	The Computer Crime Act
CCPR	United Nations Human Rights Committee
COVID-19	Coronavirus Disease 2019
CERD	Committee on the Elimination of Racial Discrimination
CRC	Cybersecurity Regulating Committee
DDoS	Distributed Denial of Service
ICCPR	International Covenant on Civil and Political Rights
ICT	Ministry of Information and Communications Technology
IOs	Information Operations
ISPs	Internet Service Providers
ISOC	Internal Security Operations Command
LGBT	Lesbian, Gay, Bisexual, and Transgender
MDES	Ministry of Digital Economy and Society
NBTC	National Broadcasting and Telecommunications Commission
NCPO	National Council for Peace and Order

NECTEC	National Electronics and Computer Technology Centre
NHRCT	National Human Rights Commission of Thailand
PDRC	People's Democratic Reform Committee
SIO	Stanford Internet Observatory
SLAPP	Strategic Lawsuit against Public Participation
TLHR	Thai Lawyers for Human Rights
TOT	Telephone Organisation of Thailand
UN	United Nations
UNHRC	United Nations Human Rights Council
UPR	Universal Periodic Review
VPN	Virtual Private Network
WGAD	Working Group on Arbitrary Detention



Executive Summary

Thailand's internet landscape is characterised by a high penetration rate and advanced infrastructure. According to the International Telecommunication Union, between 1997–2003, less than 10% of the total population had access to the internet. The number soared to 77% in 2020. Since its introduction, the internet has increasingly been used for exercising freedom of expression and promoting political mobilisation.

Today, internet freedoms in Thailand remain under threat, a product of continuous restrictions accelerated since the 2014 coup.

Legislation has been enforced to tackle expressions criticising the establishment and, as a result, to manipulate online narratives, legitimising desirable opinions about the establishment. These laws contain vague language subjected to arbitrary and extensive interpretation by the authorities and impose serious and disproportionate punishment. Non-legal measures such as fake news crackdowns and Information Operations are further adopted by the government against human rights defenders and political activists to limit their activities.

This baseline study reviews and analyses legislation that impacts internet freedoms in Thailand. These include provisions in the Constitution, Penal Code, the Computer Crime Act, the Cybersecurity Act, and the Emergency Decree. As this report shows, many provisions under these laws contain vague language enabling wide interpretation, impose harsh punishment, and give far-reaching power to the authorities.

Internet freedoms are enshrined under the Constitution. Also, Thailand has a commitment to the International Covenant on Civil and Political Rights and makes further commitments regarding internet freedom and freedom of expression via the United Nations' Universal Periodic Review process. Its current legislative and policy approach to internet freedoms falls short of its international human rights commitments.

Nevertheless, the Thai government has defended the use of these restrictions to protect and maintain national security and public order. These laws are used to justify removing or blocking content criticising the monarchy and establishment, prosecuting internet users, and harassing activists, individuals, journalists, and human rights defenders. This has led some sectors of Thai society to practise self-censorship, while others choose to defy the regime.

Recommendations on upholding internet freedom in Thailand provided in this report include: to amend or repeal provisions containing vague language and imposing harsh penalties; decriminalise defamation and place it within the civil code; and limit the application of the Emergency Decree strictly as necessary for eliminating the pandemic.

1. Introduction

In Thailand, the internet and social media have become the targets of successive juntas and military-led regimes as they have become the main political outlets through which to express critical opinions and call for reform to the existing regime. This baseline study examines the attempts by Thailand's military and their installed governments to control and manipulate expression of opinion online. It also discusses the defiance of Thais in the face of restrictions through physical protests and online civil disobedience. It outlines the use of online platforms for political expression and mobilisation and the features of the online landscape, and reviews documents submitted by Thailand to United Nations (**UN**) bodies. Thereafter, key national legislation and their relevant provisions are examined. The impact of these measures on internet freedoms and government policies to manipulate online content are then assessed. Finally, the study makes some key recommendations to promote and protect internet freedoms.

1a. Methodology

Desk research of primary and secondary documents as well as consultations with selected stakeholders were undertaken from 1 December 2021 to 31 March 2022. Primary documents include a review of UN documents from 2005 to 2021. These include documents in three of Thailand's Universal Periodic Review (**UPR**) processes in the 2011, 2016 and 2021 reporting cycles (National Reports, Stakeholder Summary, Report of the Working Group and Addendum from State under review), and documents for the State Party's report to the International Covenant on Civil and Political Rights (**ICCPR**) in the 2005, 2016, 2017 and 2021 reporting cycles. It also includes a review of national legislation that has impacted internet freedom in Thailand. Secondary documents include a review of information obtained from relevant reports of NGOs, think-tanks, government agencies and media reports to gather data and statistics on internet and social media usage, compare rankings and indices, identify human rights gaps to the realisation of internet freedoms and assess proposed solutions. Consultation calls were also set up with selected stakeholders to gather information and validate the desk research.

1b. Background

In 1997, *Pantip.com*, the first and largest online discussion forum in Thailand, was established. The *Rajadamnern* room in the forum was also one of the first open-to-all platforms for internet users to express their political views and exercise their freedom of speech. However, the direct involvement of the internet in politics began with the anti-Thaksin Shinawatra and self-proclaimed 'yellow shirt' camp in 2005. The period also coincided with a rise in blogging websites that attracted more people to the online space to express their political views, which was characterised by the political polarisation between the royalist 'yellow shirts' and the pro-Thaksin 'red shirts'. Much

of the online political discussion during the 2005–2006 political turmoil took place on forums and blogging sites such as *MThai.com*, *serithai.net*, *exteen.com*, *bloggang.com* and *OKNation.com*, in addition to *Pantip.com* (Paireepairit, 2012).

In September 2006, the military staged a coup overthrowing then-Prime Minister Thaksin and in 2007 the junta-backed interim government promulgated the Computer Crime Act (**CCA**) to criminalise the growing use of computers and the internet for political expression. As the political conflict continued in 2008, online opinion clashes between the yellow shirts and anti-coup red shirts moved from online discussion forums to rising social media platforms such as Facebook. Starting in 2009, Thailand also saw the use of social media such as Facebook and Twitter by politicians as a tool to communicate and engage with voters, inspired by the success of the then-US president Barack Obama (ibid).

Political leaders also used the internet and digital communication to mobilise their supporters directly in political protests between 2009–2014. During the 2009–2010 protests, self-exiled Thaksin adopted an online communication strategy to mobilise his red shirt supporters against military leaders and bureaucrats in monarchy networks and the military-backed Abhisit Vejjajiva (of the Democrat Party) administration. Advances in mobile technology and social media also transformed the relationship between traditional content creators and consumers. In the 2010 protests, for example, as protesters met with violent crackdowns by the army, citizen journalists used mobile technology to report on protests and the crackdowns from the front line (ibid).

The military bloc led by the Democrat Party and Abhisit was again unable to secure an electoral win in the following 2011 election, when Yingluck Shinawatra, the younger sister of Thaksin, was elected Prime Minister. Social media was then once again utilised by a political movement in 2013–2014 known as the People's Democratic Reform Committee (**PDRC**) to recruit, fundraise and mobilise support to overthrow the elected government of Yingluck (Sinpeng, 2021), criticised over her governance and links to her brother.

The military coup staged in 2014 ousted Yingluck from office and paved the way for Prayuth Chan-ocha to rule the country as the chief of the National Council for Peace and Order (**NCPO**). Under military rule, space for public opinion and political debate was curtailed. However, Thais intensified their political criticism of military rule in cyberspace (Chachavalpongpun, 2020). In response, the junta amended the CCA in 2017 delivering tougher measures curbing undesirable political expression and manipulating online narratives. This was in spite of continuing criticisms from civil society as well as recommendations from UN member states during Thailand's UPR processes to significantly repeal or amend the law.[1]

A general election was only called in 2019 after 5 years of the coup, which saw the military forming its own political party and securing a win with a coalition of military aligned parties. The 2019 election saw social media as one central political battlefield. Social media such as Facebook and Twitter functioned to disseminate news and information about the election, promote political campaigns, and determine political agendas and issues (iLaw, 2019a). The use of social media continued past the election, as it

[1] See Section 1d.

turned into a platform in which the public, especially youth, discussed politics and demanded reform.

In February 2020, a landmark decision of the Constitutional Court dissolved the pro-democracy Future Forward Party, with commentators describing the case as a grave misuse of power and an indictment of the politicised nature of the Court. Immediately following were street protests led by students and youth across the country. This time, the online space became a heated political battleground between the government and the pro-democracy movements which used the internet and social media not only to express their political demands but also to mobilise supporters to call for reforms. At the international level, the internet also provided a platform to express solidarity among pro-democracy and anti-China protesters in Thailand, Hong Kong and Taiwan. These protesters forged an online network and called themselves the 'Milk Tea Alliance' which was named after the popular and common drinks in the three countries. However, the internet is also utilised by the anti-democracy camps or state funded trolls to target and harass pro-democracy activists.

Since 1997, the online space has become an arena for political expression and after 2005, has been used by opposing camps for political mobilisation. As it has been utilised in a way that the traditional media – either controlled and monopolised by state agencies or heavily influenced by pro-regime business conglomerates – cannot serve, it has become a target of control by successive military coups and military-aligned governments.

1c. Internet Landscape

Developments in internet communications began in 1995 after an investment proposal from the National Electronics and Computer Technology Centre (**NECTEC**) to commercialise the internet service in the country was approved by the Communications Authority of Thailand (**CAT**) and the Telephone Organisation of Thailand (**TOT**). Telecommunication services were exclusively provided by state-owned telecommunications operators until they were liberalised when the Broadcasting and Telecommunication Services Act (2000) and the Telecommunications Business Act (2001) came into effect. The intention of the liberalisation was to protect the public interest and to provide a free and fair competitive environment for private Thai telecommunications businesses (Charnsripinyo & Roongroj, n.d.).

Thailand's internet growth was slow in the early years and only accelerated in the late-2010s. Between 1997–2003, less than 10% of the total population had access to the internet. Internet users increased to 15% in 2005, 39.14% in 2015, and only soared to 77.84% in 2020 (ITU, 2020), as Table 1 shows.

Table 1: Internet Users in Thailand

Year	Population (in millions)	Internet Users	
		(percentage)	(in millions)
2000	62.95	3.69%	2.32
2005	65.42	15%	9.81
2010	67.2	22.4%	15.05
2015	68.71	39.14%	26.89
2020	69.8	77.84%	54.33

(ITU, 2020 and World Bank, 2020)

Updated information from another source, We Are Social and KEPIOS, shows that in 2022, the internet penetration rate was at 77.8% with around 54.5 million users of the [2] According to a 2021 digital news report by the Reuters Institute for the Study of Journalism, 91% of Thai respondents use online media (including social media) as sources of news and information (Newman et al., 2021). 78% use at least one form of social media. Facebook is the most preferred at 66%, with Line (56%) and YouTube (53%) following suit. 47% of respondents also said that they use social media, messaging applications or email to share news (ibid.).

The internet infrastructure of Thailand is competitive as a result of continued development and investment. By 2021, there were more than 200 Internet Service Providers (**ISPs**) (Bangkok Post, 2021a). The Speedtest Global Index developed by Ookla showed that in March 2022, median mobile internet connection speed in Thailand was at 33.49 Mbps and median fixed broadband internet connection speed rose to 187.80 Mbps (Ookla, 2022). The internet infrastructure of Thailand continues to develop as the country has adopted 5G technology to upgrade mobile services and undergo the digital transformation, making Thailand the first 5G mover among the ASEAN countries.

total 70 million. Social media users in the country are at 81.2% or 56,850,000 of the total population (ibid).

Major fixed broadband providers in the country include 3BB, AIS, CAT Telecom, NT TOT and True Online. For mobile phone service, there are three major operators: AIS, owned by Thailand's Gulf Energy Development Company, Singapore Telecommunications Ltd and Temasek Holding; True Corporation, owned by the CP Group and China's state-owned China Mobile; and DTAC owned by Telenor (Tortermvasana, 2021). In November 2021, there was a merger plan of True and DTAC, followed by serious concerns that the deal would severely harm competition in the

[2] We Are Social and Hootsuite notes that the number of social media users does not necessarily represent unique individual users. In this case, the discrepancy in the total internet users and total social media users may come from one individual having one or more social media accounts.

telecommunications market. Despite opposition by customers and advocates, the merger plan of True and DTAC is likely to pass through legal and administrative checks as the telecom regulator, the National Broadcasting and Telecommunications Commission (**NBTC**) indicated it has no power to block the deal (Tortermvasana, 2022).

As of 2021, 10 International Internet Gateways are in operation in Thailand. However, the military has shown its intention to consolidate the gateways into a centralised government-controlled one. The plan, proposed in 2015, was only scrapped after fierce criticism from Thai netizens (Reuters, 2015). In 2022, the Ministry of Digital Economy and Society (**MDES**) stated in parliament that the government is reconsidering to instate a national internet gateway. Along with considering amending the CCA, the government is studying the possibility of using a single internet gateway with the aim of tackling cyber criminals overseas, controlling the flow of illegal information online and improving the safety of internet users (Bangkok Post, 2022).

1d. Adherence to International Human Rights Standards

In this section, the degree to which internet freedoms are upheld in Thailand is evaluated through Thailand's adherence to international human rights standards reported in documents from various UN human rights mechanisms. These include Thailand's UPR processes in 2011, 2016 and 2021 and the country's submissions to the ICCPR treaty body in 2004 and 2015. At the regional and national level, the significance of the Association of Southeast Asian Nations (**ASEAN**) Human Rights Declaration (**AHRD**), ASEAN Intergovernmental Commission on Human Rights (**AICHR**), and the National Human Rights Commission of Thailand (**NHRCT**) are also briefly considered.

1di. International Human Rights Mechanisms

Thailand is a party to international treaties creating international legal obligations. Directly concerning internet freedoms is the ICCPR it acceded to in 1996. Article 19 of the ICCPR ensures the protection of free speech across all mediums: 'either orally, in writing or in print, in the form of art, or through any other media of his choice' (ICCPR, 1966).

The article is further clarified by the Human Rights Committee under the Covenant in its General Comment No. 34 as aiming to ensure the protection of all forms of expression and the means of their dissemination, including audio-visual as well as electronic and internet-based modes of expression. A positive interpretation of the term 'protection' by the Committee also requires that states parties encourage the independence of new media and ensure access to it. The Committee also states that Articles 19 and 20 of the ICCPR are compatible with and complement each other. Article 20 provides that propaganda advocating war or national, racial or religious hatred is prohibited by law (UNHRC, 2011a).

In its latest General Comment regarding Article 21 (right to peaceful assembly), the Committee raised the fact that the online space should be considered no different from physical space insofar that it is where citizens can express their opinion and peacefully assemble to do so. To this end,

states parties should ensure that peaceful assemblies are protected wherever and however they are held: in person or remote (online). Furthermore, states must not block or hinder internet connectivity in relation to peaceful assemblies or apply geo targeted or technology-specific interference; this also applies to ISPs and intermediaries (UNHRC, 2020a).

Freedom of opinion and expression form a basis for other human rights. The rights to free expression, opinion, information and privacy often engage with the rights to peaceful assembly, freedom of association and political participation within the online sphere. The rights to freedom of association, peaceful assembly and political participation are guaranteed respectively under Articles 21, 22 and 25 of the ICCPR. Article 22 ensures the right to freedom of association and to join a trade union, while Article 25 entitles the right to participate in public affairs, to vote and to be elected and access to public service.

However, there are some permissible limitations on these freedoms defined in ICCPR. Some Articles of the ICCPR allow restrictions provided that they are provided by law and as necessary for national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others. In addition, in times of public emergency, Article 4 of the Covenant allows the states parties to derogate from ICCPR obligations including Article 19, 20, 21, 22 and 25 as required by the exigencies of the situation (ICCPR, 1966). The Committee further emphasises in General Comment 29 that the rights of derogation are very narrow and the emergency measures must be strictly proportionate to the danger (UNHRC, 2001).

Thailand has been slow to submit ICCPR state party reports. It submitted a report for the 1998 cycle in 2004 and for the 2009 cycle in 2015. In the concluding observations of the Human Rights Committee dated 8 July 2005, the Committee raised concerns over reports of intimidation and harassment against local and foreign journalists and media personnel as well as defamation suits against them. The Committee recommended Thailand take measures to prevent further erosion of freedom of expression, in particular, threats to and harassment of media personnel and journalists (CCPR, 2005).

For the second ICCPR reporting cycle, in the 2015 state party report, the importance of freedom of expression was recognised and Thailand presented provisions implemented to protect them. However, the Government claimed that while certain laws have infringed the people's freedom of expression, these laws were being applied cautiously by the authorities. It also defended the use of the lèse-majesté law as necessary to protect both national security and the highest institution of Thai society. Meanwhile, the CCA was described as enacted to more effectively deal with a range of criminal activities committed via computers and the internet (CCPR 2015).

In concluding observations of the Human Rights Committee (**CCPR**) dated 25 April 2017, the Committee welcomed the submission of the second period report of Thailand, albeit six years late. It expressed concern about reports of the severe and arbitrary restrictions imposed on the right to freedom of opinion and expression in national legislation, including in the Penal Code and the CCA. It recommended that Thailand take all measures to guarantee the enjoyment of freedom of opinion and expression and refrain from using its criminal provisions, including the CCA, the sedition law and others, as tools to suppress the expression of critical and dissenting opinion (CCPR, 2017). In a 2020 follow-up report to its concluding

observations, the Committee stated that the Thai Government had not yet taken any specific measures to implement the Committee's recommendation on the Constitutional and legal framework to uphold fundamental rights of people (CCPR, 2020).

Thailand has also participated in the UPR processes in 2011, 2016 and 2021. As early as the first UPR cycle, concerns were raised over continued restrictions on freedom of expression and opinion in Thailand. The UN compilation document (UNHRC, 2011b) and the stakeholder's compilation (UNHRC, 2011c) highlighted the high profile case of Ms. Chiranuch Premchaiporn (*Prachatai.com's* webmaster who was charged under the CCA for not removing online anti-monarchy comments from the website) and the shutting down of several websites for allegedly promoting anti-monarchy sentiments and posing threats to national security. The Thai government responded during the UPR that it attached importance to the right to freedom of opinion and expression which it regarded as the bedrock of Thailand's democratic society; nevertheless, that it strived to strike a balance between protecting the monarchy and exercising people's freedom of expression. It further clarified that governmental agencies regularly review relevant legislation to make recommendations to the government and provide legal advice to the police and prosecutor on instituting legal proceedings under the Penal Code and CCA (UNHRC, 2011d).

During Thailand's second UPR cycle, the compilation of UN information (UNHRC, 2016a) noted that orders issued by the NCPO[3] were aimed at curbing press freedom and freedom of expression, including by closing down anti-junta media and websites as well as restricting freedom of assembly and association. Meanwhile, the stakeholder summary (UNHRC, 2016b) highlighted ongoing patterns of media censorship, restrictions on the media, harassment and detention of media workers and self-censorship by the media as a result of tough provisions adopted by the Thai authorities. In this cycle, the Thai government once again stressed their respect for freedom of opinion and expression and freedom of assembly as a basic foundation of a democratic society. However, consistent with its response during the first cycle, the government affirmed that freedom of expression must be exercised in a constructive manner, in an appropriate context, and without insulting any faith or belief system or disrupting social order and security (UNHRC, 2016c).

In the third UPR cycle (2021), the CCPR's concerns over the severe and arbitrary restrictions of freedom of expression and criminal proceedings, especially criminal defamation charges, brought against human rights defenders, activists, journalists and other individuals were noted in the compilation of UN information (UNHRC, 2021a). Moreover, concerns were raised over freedom of expression issues related to COVID-19 and the anti-fake news centre established under the MDES. The stakeholder summary also highlighted various stakeholders' concerns about restrictions on freedom of opinion and expression in the country through vaguely worded legislation inconsistent with international human rights standards (UNHRC, 2021b). In this cycle, the Thai government reaffirmed its commitment to respect and protect freedom of expression

[3] The National Council for Peace and Order (NCPO) was the military junta established for the military coup in May 2014 and ruled Thailand between 2014-2019. NCPO was the 13th revolutionary committee in Thailand and had the legal status of sovereignty under Thai law during the period it ruled. It consisted of all branches of the armed forces and the police.

and freedom of the media but added that it was mindful to ensure that the exercise of freedom of expression must be done in a constructive and appropriate manner (UNHRC, 2021c).

The major point of contention related to internet freedoms across Thailand's three UPR cycles were:

- The vaguely worded legislation inconsistent with international human rights standards including Article 112 (lèse-majesté), 116 (sedition), 326 (defamation), 328 (libel) of the Penal Code, the CCA (2007), NCPO orders, criminalisation of defamation and Section 44 of the interim Constitution which are utilised by the authorities to limit freedom of expression and opinions in the digital space.
- Strict measures under the Emergency Decree for Public Administration in Emergency Situation (2005) that restricted the right of peaceful assembly and to information.
- The dramatic increase in arbitrary detentions and prosecutions against people for lèse-majesté crimes with harsh punishment since the military coup.
- States Parties' recommendations to repeal or amend restrictive legislation including provisions of the Penal Code and the CCA that impacted on internet freedoms; and the government's consistent response that the law is not aimed at curbing people's rights to freedom of expression or academic freedom but for the protection of national security and the highest institution of Thai society.

1dii. Regional Human Rights Mechanisms

Thailand adopted the AHRD in 2012 and affirmed its commitment to implementing the AHRD to promote and protect human rights. Internet freedoms and freedom of expression are upheld by Article 23 of the AHRD stipulating that 'every person has the right to freedom of opinion and expression, including freedom to hold opinions without interference and to seek, receive and impart information, whether orally, in writing or through any other medium of that person's choice' (AHRD, 2012). However, AHRD is not legally binding; therefore, there is no mandate to force the state parties to implement it.

Thailand also has fully supported the work of the AICHR. During its ASEAN chairmanship in 2019, Thailand led the initiation of a timely review of the Terms of Reference of the AICHR to better respond to evolving human rights situations. At present, AICHR itself has more promotion activities, rather than protection activities such as receiving complaints against human rights violations and providing remedies (Muntarbhorn, 2021). Moreover, a key problem of this mechanism comes from the appointment of 'state connected' individuals as AICHR representatives by a majority of the governments, which impedes real independence (Gomez and Ramcharan, 2018). In May 2018 the ASEAN Ministers Responsible for Information (**AMRI**) declared a framework and joint declaration to minimise the harmful effects of fake news. The framework outlined four broad strategies for the member countries to use in addressing online fake news – education and awareness, detection and response, norms and guidelines, and community and ground-up participation. However, the framework was silent on addressing falsehoods put out by government leaders and officials, especially in attacks against their critics (Gomez, 2018).

1diii. National Human Rights Mechanism

The NHRCT was first established as a non-governmental Constitutional agency under the 1997 Constitution as an independent organisation to promote and protect the rights and liberties of the people.

Pursuant to the duties and powers as specified in the Organic Act on the National Human Rights Commission (2017), the NHRCT regularly publishes its assessment on Thailand's human rights situation. The 2020 assessment report referred to a case when the authorities issued an order under the Emergency Decree to investigate and suspend four online media outlets including Voice TV, Prachatai, The Reporters, and The Standard, as well as the Facebook page of the student activist group Free Youth in October 2020. Nevertheless, the NHRCT was only able to comment and suggest to the government that measures during the emergency situation must comply with Article 4 of ICCPR by adhering to the legal principles of necessity, proportionality and non-discrimination (NHRCT, 2020a).

In addition, it commented in its summary investigation report no. 89–97/2021 regarding freedom of assembly during the political protests between July and December 2020 that online and social media operations undertaken by authorities during the political protests – widely regarded as a breach of freedom and privacy[4] – were lawful. The operations in question included collecting evidence, requesting for court orders to suppress dissemination or remove the computer information of individuals or private organisations that supported the demonstration and closely monitoring social media accounts that posted allegedly inappropriate pictures and contents. NHRCT was only able to warn that these operations may affect freedom of expression or the right to access information and recommend that the authorities should carry out operations only as necessary and not enforce the law discriminately against the protesters based on differences in political opinions (NHRCT, 2020b). These actions were severely lacking, considering the abuse of human rights that were taking place.

Yet in a divergent reaction to its national reports, the NHRCT's submission to the UN Human Rights Council (**UNHRC**) during the 2021 third cycle of the UPR process expressed substantive concern about law enforcement against online media users including via the CCA. The Commission recommended such measures be implemented with extreme caution, not to intrude into people's right to privacy or limit their freedom of expression. It also recommended that the authorities should consider the principle of legality in enforcing these laws (NHRCT, 2021).

During the same UPR process, UN agencies raised concern over the lack of a clear, transparent and participatory process for selecting and appointing members of the NHRCT, causing a downgrade to grade 'B' in November 2015 as credited by the Global Alliance of National Human Rights Institutions (UNHRC, 2021a). During the cycle, CSOs also reported the NHRCT's inability to monitor and investigate human rights violations (UNHRC,

[4] In October 2020, the authorities shut down four online media for violating the CCA and Emergency Decree. However, the order was later overturned by the Criminal Court. The Court stated that the online media outlets enjoyed the protection under Section 35 of the Constitution citing that a media professional shall enjoy the liberty to present news or express opinions in accordance with professional ethics and the closure of a newspaper or other mass media in deprivation of the liberty under paragraph one shall not be permitted. (Prachatai, 2020a).

2021b). A report in 2020 by the Asian NGO Network on National Human Rights Institutions (**ANNI**) similarly pointed out that the NHRCT's independence was threatened due to flaws in the appointment and selection process (Forum-Asia, 2021) and that it fails to uphold human rights in the context of the pandemic and the mass protests.

Having outlined Thailand's political background, internet landscape and position relative to its commitments under the international, regional and national mechanisms, the next chapter will explore the legal framework of the country. It will outline the relevant provisions including the Constitution of Thailand, the Penal Code, the CCA, and the Emergency Decree and consider how these restrictive laws threaten internet freedom in contradiction to its international human rights obligations.

2. Laws

A range of freedoms are guaranteed under the Thai Constitution, but they are restricted by limitations inconsistent with international standards. Internet freedoms especially are restricted through vaguely worded provisions in the Penal Code, the CCA, the Cybersecurity Act and the Emergency Decree that can be arbitrarily interpreted by government authorities. This chapter reviews these laws by examining the relevant provisions and highlighting the applicable penalties for the infringements.

2a. Constitution

Having gone through 19 constitutions after military coups in less than a century since the revolution in 1932, Thailand officially promulgated the current 20th Constitution in April 2017 backed by the junta and with negligible civil society and public participation during its drafting (Head, 2017). During the constitutional referendum, relevant debates and campaigning were suppressed and activists were prosecuted as they advocated for Thais to reject the draft Constitution (UNHRC, 2021a).

Internet freedoms are not directly specified in the Constitution. However, freedom of expression, academic freedom, freedom of the media and the right to privacy are guaranteed. However, these Articles contain limitations framed in vague and overly broad ways and open to expansive interpretation by the authorities.

Freedom of expression is guaranteed under Article 34 of the Constitution. The Article provides that 'a person shall enjoy the liberty to express opinions, make speeches, write, print, publicise and express by other means' and restricted only by laws specifically enacted for 'the purpose of maintaining the security of the State, protecting the rights or liberties of other persons, maintaining public order or good morals, or protecting the health of the people'[5]. Academic freedom is constitutionally restricted to not be 'contradictory to the duties of the Thai people or good morals, and [to] respect and not obstruct the different views of another person' (Constitution of Thailand, 2017).

Based on Article 19 of the ICCPR, restrictions on freedoms of expression are permitted as provided by law and necessary to respect the rights or reputations of others and to protect national security, public order, public health or morals. However, the CCPR's General Comment no. 34 also clarifies that these restrictions must not be overbroad and must further conform with proportionality. Article 34 of the Constitution defines legitimate limitations that may be placed around freedom of expression that are broadly consistent with the ICCPR. In practice, however, the authorities have arguably interpreted these limitations in precisely the sort of overbroad manner

[5] Based on Article 19 of ICCPR, restrictions on freedom of expression are permitted only to respect the rights or reputations of others and to protect national security or of public order or of public health or morals. However, the restriction must be provided by law and be necessary. General Comment no. 34 also stated that restrictions must not be overbroad and must conform to the principle of proportionality.

against which General Comment no. 34 cautions.

As for the freedom of the media, while it is upheld under Article 35 of the Constitution, such freedoms are conditioned to the adherence to professional ethics. Article 35(1) states: 'A media professional shall enjoy the liberty to present news or express opinions in accordance with professional ethics'. In January 2022, the government proposed and subsequently passed the draft 'Media Ethics and Professional Standards Promotion Act', which is now before the parliament. This law intends to set up a state-operated Media Council to institutionalise the constitutional obligation to maintain the 'professional ethics' of the media (Khaosod English, 2022) .

The Article also specifies (35(2)) that arbitrary shutdowns of media organisations (provided they adhere to the first clause) is not permitted. However, it allows for prior censorship of the media during states of war (35(3)) and restricts the ownership of media to Thai nationals (ibid).

The right to privacy is assured under Article 36 regarding the freedom of communication. As part of such freedom, the Article stipulates that the act of disclosure of communications between individuals is prohibited and allowed only by a Court order or warrant, or where there are other grounds as provided by other laws (ibid).

2b. Penal Code

Provisions under the Penal Code (1956) imposed to curb the rights to freedom of opinion and expression which are of concern to internet freedoms in the country include, among others: Article 112 (lèse-majesté), Article 116 (sedition) and defamation charges (Article 326–328). Furthermore, its consecutive sentencing approach is also used to aggravate punishment.

Article 112 (lèse-majesté) of the Penal Code criminalises '*whoever defames, insults, or threatens the King, the Queen, the Heir-apparent of the Regent with imprisonment of three to fifteen years*' (Penal Code (1956). Article 112's problems arise from its vague legal provision and enforcement. Under this provision, the act of 'insult' is not specified and is subjected to vague and nebulous interpretations by the authorities. A review of recent use cases of Article 112 also shows a precedence of a minimum sentence of 5 years per count (iLaw, n.d.). Moreover, since anyone can accuse anyone else under the law, the Article is widely used, including via complaints filed by royalists as private citizens, to prosecute anyone perceived as failing to respect the monarchy, a grave offence in Thai culture.

Article 116 (sedition) of the Penal Code criminalises '*anyone who use words, writings or any other mean beyond the purpose of the Constitution or not for expressing an honest opinion or criticism in order to bring about a change in the Laws of the Country or the Government by the use of force or violence; to raise unrest and disaffection amongst the people in a manner likely to cause disturbance in the country; or to cause the people to transgress the laws of the Country*' with imprisonment no more than 7 years (Penal Code (1956). The Article again contains vague terms that can be interpreted arbitrarily by the authorities. For example, it does not specify what kind of action shall be considered to 'raise unrest and disaffection amongst the people'.

Defamation is criminalised under the Penal Code in addition to the Civil Code. The provisions include:

- Article 326 criminalising defamation 'with imprisonment not exceeding one year or a fine not exceeding THB 20,000 [USD 595], or both';
- Article 327's stipulation that 'anyone who imputes the deceased person and that imputation causes the father, mother, spouse or child of the deceased to be hated or scammed shall be punishable as prescribed by [Article] 326'; and
- Article 328 criminalising 'defamation committed by means of publication with imprisonment not exceeding two years and fine not exceeding THB 200,000 [USD 5945]' (Penal Code (1956)).

In practice, these defamation laws have been abused as tools to silence and punish government critics, activists and journalists (Bangkok Post, 2019). These provisions are also frequently used by the private sector and government in the form of Strategic Lawsuits Against Public Participation (**SLAPPs**)[6] and judicial harassment against dissenting voices – usually towards human rights defenders.

Provisions under the Thai Penal Code curb the rights to freedom of opinion and expression in Thailand. They contain overbroad language at risk of arbitrary interpretation and impose harsh punishments, not aligning with Thailand's commitments under international human rights law.

2c. The Computer Crime Act

In 2007, the CCA was introduced by the junta-backed government of General Surayudh Chulanont. It was enacted at a time when the availability and usage of internet services were becoming widespread among Thai people (Charoen, 2013) in order to tackle cybercrimes and silence critical opinions against the junta. In December 2016, its amendment was adopted by the Prayuth junta-appointed National Legislative Assembly and put into force in 2017 to address the problems with the enforcement of law. The problems addressed were twofold; first, that the law was applied to 'security' offences more than hacking offences and second, that it provided insufficient power for the authorities in seeking out those who committed online offences and in controlling harmful content (iLaw, 2016). Overall, the amendment of the CCA enhanced sentences and created a series of overlapping offences with subsections, added more vague language and increased censorship.

The CCA, containing a total 31 provisions can be divided into three major parts: general provisions (Section 1 - 4), offences (Section 5 - 17) and competent officials (Section 18 - 31). Section 14, 15, 18, and 20 will be reviewed in this part since they have become contentious for their effect, in practice, of restricting freedom of expression.

[6] To deal with SLAPPs, in 2018 the National Legislative Assembly of Thailand amended two provisions of the Criminal Procedure Code. Section 161/1 was amended to authorise courts to dismiss cases filed by private parties with the intention to harass or take undue advantage of a defendant or to procure any advantage to which the complainant is not rightfully entitled. Also, Section 165/2 was amended to allow defendants to submit evidence during a preliminary hearing showing that a case lacks merit.

Article 14 of the CCA stipulate up to five years of imprisonment or a fine of no more than THB 100,000 (USD 2,972) or both, for 'entering … distorted or false computer data … deemed to cause damage to the general public, national security, public safety, economic safety or to cause panic to the general public'. This includes the crime of 'disseminating or forwarding such computer data' (Computer Crime Act, 2017). However, this Article does not provide a clear definition of what is distorted or false information and does not specify what kind of information that can cause damage.

Under Article 15, 'a service provider, who cooperates, consents or supports the perpetration of the offences' is liable for the same penalty as the offender under Section 14 of the Act. In this case, the MDES can issue a notification specifying the process of warning, blocking the dissemination and removal of such computer data (known as the 'notice and takedown mechanism') (ibid).

Section 18 specifies that officials under the Act have power to:

- request statements from those related to the perpetration of an offence (sub-section 1); to request computer traffic data from service providers (sub-section 2);
- order service providers to submit information relating to their clients (sub-section 3);
- duplicate computer data and computer traffic data from computer system suspected of being used for an offence (sub-section 4);
- order the computer data processor or controller or those who own storage devices to deliver such computer data or devices (sub-section 5);
- inspect or access computer system, computer data, computer traffic data or storage device of anyone as evidence related to the offence (sub-section 6);
- decode computer data of anyone (sub-section 7); and
- seize or attach any computer system for purposes of investigation and evidence gathering (sub-section 8).

Section 20 provides that the official, with approval from the Minister, may file a petition to the court to stop dissemination or to remove data in question. Such power applies to any computer data that compromises the security of the country, relates to other criminal laws and breaks the public order or good morals. In an action that is deemed to be a breach to the public order or good morals of the people, the Minister has the power to file a petition to the court to suppress the dissemination or to remove the computer data (ibid).

Finally, Section 27 stipulates that 'whoever fails to comply with an order of the court or the competent official pursuant to Section 18 or Section 20 … shall be liable to a fine not exceeding THB 200,000 [USD 5,945] and a daily fine not exceeding THB 5,000 [USD 148] until the order is properly complied with' (ibid).

The CCA is intrinsically problematic. Its provisions contain vague language that are subject to varied interpretation and discretion of the authorities. Furthermore, it is implemented selectively to block or remove undesirable content and prosecute individuals who express opinions against the establishment or monarchy. Often, the Act is used by the authorities to harass internet users and create an atmosphere of fear, leading to self-censorship.

2d. The Cybersecurity Act

The Cybersecurity Act was unanimously approved by the junta-appointed National Legislative Assembly and entered into force in 2019. The Act can be divided into four major chapters: the Committee, the Office of the National Cybersecurity Committee, maintaining cybersecurity, and penalty provisions. A cyber threat is defined in Section 3 of the Act as any action by using a computer, computer system, or undesirable programme with an intention to cause any harm to the computer system, computer data or other relevant data (Cybersecurity Act, 2019).

Such definition regards crimes under the Act as involving only the act of using computers and programmes to cause harm to other computers or data – a threat under this Act, then, is not based on content that was put into the system. Therefore, expressions or opinions cannot be considered as cyber threats. However, since the definition of these threats do not explicitly rule out the posting of comments and opinions, the vagueness of the law nevertheless enables the Act to be interpreted arbitrarily by the authorities and expanded to cover expressions and opinions. The issue of interpretation arises in Article 60 of the Act, categorising cyber threats into three levels: non-critical, critical and crisis. At the crisis level are cyber threats that 'affect or may affect the public order or is a threat to public security'. iLaw (2019b) notes that since a cyber crime at this level is defined in terms of its effects, rather than the nature of the crime, it creates space for expanding the offence to also include content put into the computer or put online.

Furthermore, officials under the Act are given extraordinarily vague powers at risk of overbroad interpretations. Article 66 of the Cybersecurity Act provides that in preventing, coping with, or mitigating the risks from cyber threats in a critical level, the Cybersecurity Regulating Committee (**CRC**) has the power to:

- order an official to enter into a suspected place of operation (subsection 1);
- access the computer data, computer system and copy or filter/screen data which there is reason to suspect is related to the cyber threat (subsection 2);
- test the operation of a computer deemed to be related with or affected by the Cyber Threat or used to search any information from the inside or to take advantage of the computer (subsection 3); and
- seize or freeze a computer or any equipment, only to the extent it is necessary, which there is a reason to suspect is related to the Cyber Threat for the examination or analysis, for not more than 30 days (subsection 4) (ibid.).

Section 76 of the Cybersecurity Act states that any person disrupting or not complying with an orders of the CRC or not complying with the Court order in accordance with the Act without a reasonable cause will be subject to imprisonment not exceeding three years, a fine not exceeding THB 60,000 (USD 1,783.), or both (ibid).

The Cybersecurity Act gives the government far reaching powers to monitor online information, access computer data and seize electronic or computer equipment. Since the Act contains vague language, it is open to wide interpretation by the authorities.

2e. The Emergency Decree and Related Administrative Orders

In 2005, the Emergency Decree on Government Administration in States of Emergencies (the **Emergency Decree**) was enacted by then-Prime Minister Thaksin and was implemented in the three southern provinces of Thailand as a response to the prolonged conflict in the region. The Decree gives power to the Prime Minister to declare a state of emergency in some parts of the country or nationwide and to issue regulations to limit people's rights and freedoms. It also authorises the Prime Minister during an emergency to override the authority of any government ministry or agency, civilian or military, with such authorities free from supervision of the country's Administrative Court and the Court of Justice.

The Emergency Decree has been mostly enforced to address the ongoing violence in the southern provinces. The Decree was also regularly declared in Bangkok and other provinces in the political turmoil of the military coup in 2006, the red shirt protest in 2009 and 2010, and PDRC protest during 2013–2014. In March 2020, a state of emergency under the Decree was declared nationwide in response to the COVID-19 pandemic and anti-government protests (Samabuddhi, 2021). Article 18 of the Emergency Decree provides that '*any person who violates a Regulation, Notification or order issued under [the Decree] shall be liable to imprisonment for a term not exceeding two years or to a fine not more than THB 40,000* [USD 1,188] or to both' (ibid.).

Under the government of Prayuth, the Emergency Decree was extended across the country to curb the COVID-19 pandemic, for consecutive for two month-periods over a total of two years. In July 2022, the Emergency Decree was extended for the 19th time and effective until 30 September 2022 (Thai PBS World, 2022).

Moreover, in October 2020, the government declared a 'severe state of emergency' under Section 11 of the Decree in all areas of Bangkok in response to rising pro-democracy protests (Strangio, 2020). The government claimed that the October rallies threatened national security, affected the safety of the public and deteriorated measures to curb COVID-19 (Declaration of a Serious Emergency Situation, 2020). The declaration was lifted a week later.

Article 9(3) of the Emergency Decree further provides that 'in the case of necessity in order to remedy and promptly resolve an emergency situation or to prevent the worsening of such situation, the Prime Minister shall have the power to issue the Regulations in order to prohibit the press release, distribution or dissemination of letters, publications or any means of communication containing texts which may instigate fear amongst the people or is intended to distort information which misleads understanding of the emergency situation to the extent of affecting the security of state or public order or good moral of the people both in the area or locality where an emergency situation has been declared or the entire Kingdom' (Emergency Decree, 2005). This law contains vague and overly broad language such as 'instigating fear amongst the people' or 'affecting the security of state or public order or good morals of the people'. It is open to extensive and arbitrary interpretation by the authorities.

On 25 March 2020, Regulation No. 1 under Section 9 of the Emergency Decree was issued by the Prime Minister. Under the

Regulation, 'presenting or disseminating news through any media featuring content on the COVID-19 which is false or may instigate fear among the people, or to intentionally distort information which causes misunderstanding of the emergency situation to the extent of affecting the public order or good moral of the people, shall be prohibited'. The Regulation also provides that 'officials shall issue warnings to cease such mentioned acts or order to correct such news, or in cases where there are severe impacts, shall instigate a proceeding in accordance with the CCA or the [Emergency Decree]' (Regulation under Emergency Decree (no.1), 2020).

As the anti-government protests continued, in October 2020, the Commissioner General of the Royal Thai Police issued Announcement no. 4 pursuant to Article 9 of the Emergency Decree stipulating that 'audio transmitters, mobile phones, communication devices, electronic devices, or other devices that can present news, or distribute pictures, sounds or messages which may instigate fear amongst the people or is intended to distort information which misleads understanding of the emergency situation to the extent of affecting the security or state or public order or good moral[s] of the people throughout the Kingdom shall not be permitted' (Thaipbs, 2020). It also provides that 'anyone who violates this Announcement shall be liable to imprisonment for a term not exceeding two years or to a fine not more than THB 40,000 [USD 1,188], or to both'.

On 29 July 2021, Regulation no. 29 was issued under Article 9 of the Decree in the face of mounting criticism of the government's handling of the pandemic and vaccination programmes. The regulation empowers the country's National Broadcasting and Telecommunications Commission (**NBTC**) to cut internet access of social media users posting content that may frighten people. However, the Regulation was revoked in August 2021 after the Civil Court issued an injunction. This move came after the Human Rights Lawyer Alliance and 12 media companies filed a complaint against the Prime Minister Prayuth as the head of the Centre for Covid-19 Situation Administration, asking the court to revoke the 29th regulation. The Civil Court issued an injunction that suspended the regulation. In a statement, the court announced that the regulation went against the law and existing legal instruments can be used to address illegal dissemination of information (Bangkok Post, 2021).

The Emergency Decree gives the authorities sweeping and unchecked powers with negative impact on internet freedoms. It contains overbroad language that can easily be arbitrarily interpreted by the authorities to penalise critics. Also, officials carrying out duties under the decree also enjoy legal immunity. Section 17 of the Emergency Decree grants legal immunity to those in power acting in good faith. This Section exempts all regulations, announcements, and notifications from judicial review. Those who are adversely affected by the performance of the officials cannot access remedies except through civil torts. This violates Thailand's ICCPR obligation to provide access to effective remedies (Destination Justice et al, 2021).

Laws that impact internet freedoms contain restrictive provisions with language and wordings open for wide interpretation by authorities and impose tough penalties. These laws are not aligned with international human rights standards and can be open to political abuse. The next chapter shows that the laws are currently being utilised as a tool to limit critical political opinion and to limit mobilisation, which in turn impacts internet freedom in Thailand.

3. Impact on Internet Freedoms

Following a review of the different legislation, this chapter evaluates their impact on internet freedoms in Thailand. From removing content and blocking access to shutting down and slowing access to social media platforms, these laws have had a significant impact on Thai citizens' internet freedoms. It should also be noted that the government uses a mixture of measures that range from removing and blocking content to prosecuting those who posted or shared content over social media. The consistent, overarching aim is to control the online narrative. Such measures outlined in this chapter lead to an increase in self-censorship in some and prompt acts of defiance against the establishment in others.

3a. Removing and Blocking Content

Almost all popular online platforms have received orders to remove and/or block access to contents that is deemed unlawful. Article 15 and 20 of the CCA compels technology companies to remove and block online as directed by the relevant government authorities. Most of the targeted content and sites related to criticisms against the government and monarchy as well as for political mobilisation.

In 2022, Google received 1,147 requests from the Thai government and agencies to remove content since 2011 with 95.2% (around 1,092 requests) relating to government criticism. A study by Surfshark, a virtual private network (**VPN**) firm, which analysed Google's Transparency Report, revealed that for 2020 alone, Thailand submitted 184 requests for content removal. The country is 16th in Google's global total removal rankings in 2021 (Leesa-Nguansuk, 2022). For YouTube, between July to September 2021, 163,800 videos were removed from the platform as requested by the Thai government, making the country 8th in the global removal rankings (Google, 2021).

Information from Facebook's Transparency Center revealed that between January to June 2021, Facebook restricted access to 628 items in Thailand as requested by the MDES for allegedly violating the lèse-majesté law. Previously, between July to December 2020, the centre reported that Facebook had restricted access to 1,746 items in Thailand as requested from MDES, of which 1,745 items contained content allegedly violating the lèse-majesté law. Facebook had also restricted access to 1 reported as locally unlawful hate speech (Facebook, 2021).

In one of the government's requests, Facebook was compelled to block the 'Royalist Marketplace' Facebook group with 1 million members critical of the country's monarchy. In response, Facebook threatened to sue the Thai government. It said in a statement that the request breaks international human rights law, and causes a chilling effect on people's ability to express opinions (Iyengar, 2020b). This was a very rare move for Facebook as the platform

rarely diverges from government policies and national laws.

Twitter reports that from January 2012 to June 2021, it received a total 103 information requests by the Thai authorities. Total compliance, however, stands at 0. During January–June 2021, Twitter received 34 information requests from the Thai authorities, increasing from July–December 2020 when there were 22 information requests. The report also shows that from January 2012 to June 2021, Twitter received 191 requests from the Thai government to remove or withhold content. Total compliance rate of removal actions is at 12.1%.[7] Between January–June 2021, Twitter received 78 legal demands to remove or withhold content by the government (Twitter, 2021).

In June 2021, internet service providers were reminded by MDES to follow a court order to restrict access to or delete computer data of 8 allegedly illegal users on Facebook within 24 hours. Facebook accounts targeted by the Minister were those known to be critical of the monarchy, including Pavin Chachavalpongpun, Andrew MacGregor Marshall, the group 'Royalist Marketplace-Talad Luang', Suda Rangkupan, DK Ning, Aum Neko, the page 'KTUK – Thais in UK', and the page 'Pixel HELPER' (Prachathai, 2021a).

As the anti-government movement escalated, in October 2020, the country's ISPs and mobile network providers were ordered by the Thai government to block access to different websites and programmes. Access to the online petition site *Change.org* was also blocked. This was a result of a petition in the website that called for King Maha Vajiralongkorn to be declared *persona non grata* in Germany.[8] The petition drew nearly 130,000 signatures before the site was blocked. MDES stated that the petition's contents violated Thailand's CCA. The Thai Netizen Network, a group promoting internet freedom, noted that the blocking of the web was done by TOT Public Company, a state-owned telecommunications company (Khaosod English, 2020). In addition, at the peak of demonstrations in October 2020, the Thai authorities planned to block Telegram, which was a very popular and secure messaging app used by activists to mobilise their supporters (BBC, 2020). The top-secret notice ordering internet service providers to block Telegram was leaked and then reported by the media. However, the move was abandoned after the leaked document faced strong criticism.

There were also cases of mobile cut-offs and platform shutdowns. Apart from silencing critics, it was also noted that they were part of the Government's surveillance operations. At 3:35 PM on 28 May 2014, six days after the military coup launched against the then-

[7] While there are no official reasons given why it preferred not to comply with demands from the Thai government, the platform outlines how it processes requests. First, a legal request is submitted via email, mail, fax, or its legal request submissions site by law enforcement, a government agency, a lawyer representing a criminal defendant, or a civil litigant. Next, a Twitter agent will review the legal request to determine whether it meets requirements. The agent will examine the reported account or Tweets for any indications that the request seeks to restrict or chill freedom of expression; raises other Twitter policy concerns or raises practical or technical concerns. In the third step, Twitter will attempt to notify the reported account holder(s) of the existence of a legal request pertaining to the account(s). In the last step, the Twitter agent then applies its company policies for handling legal requests. This implied that in response to the government's request, Twitter set a transparent process, and concerned with key indicators.

[8] Dr. Pavin Chachavalpongpun, an exiled scholar at Kyoto University, explained that based on hearsay, King Vajiralongkorn began living in Germany in 2007. Since becoming sovereign, the King has continued to spend most of his time in Germany, usually at his lakeside villa in Tutzing, in Bavaria (Weedon, 2021).

Prime Minister Yingluck, Facebook was shut down in Thailand for 30 minutes. The Permanent Secretary of the Ministry of Information and Communications Technology (**ICT**) claimed that the social network was temporarily shut down to prevent anti-military protests. However, research carried out by Privacy International analysed that the government actually attempted to surveil online communications and rather than censor Facebook users (Privacy International, 2017).

In addition, from 2019, residents in the three of Thailand's Southern Border Provinces and some districts of Songkhla were required by the Thai government to re-register their SIM cards with their fingerprints and facial image. Local people who refused to submit their biometric data were threatened with having their mobile services cut (Chandran, 2021). The biometric registration implemented in the region was based on the orders issued by the NBTC, Section 16 of the Internal Security Act (2008) and Section 11 (6) of the Emergency Decree. The Committee on the Elimination of Racial Discrimination (**CERD**) expressed concerns in the concluding observations about the reports of SIM card registrations which was motivated by surveillance purposes, identity checks and arrests of members of ethnic and ethno-religious groups carried out on the basis of racial profiling (CERD, 2022). As of 2019, there were reportedly 1,500,000 SIM card users in the southern border provinces, including 300,000 monthly registration SIM users. The Region 4 Forward Command of the military's Internal Security Operations Command (**ISOC**), which is established to resolve the situation in the deep South of Thailand, revealed in 2020 that 888,813 mobile numbers had completed the SIM card registration (Dina, 2020).

Almost all popular online platforms used by Thai people as sources of news and information have been requested to remove content that is undesirable to the monarchy and military-backed government. MDES is a key player in submitting requests to the courts to issue orders to block and remove online content. After the courts issue an order, authorities will either block access or remove content themselves, or order ISPs to comply with the court order, and send the order to the NBTC to duly instruct ISPs and telecommunication companies. Thailand also experienced mobile cut-offs and platform shutdowns in 2019 and 2014. These measures, justified by the national legislation, are attempts by the government in keeping the online content under surveillance.

3b. Prosecuting Users

A range of critics as well as those who use internet platforms to mobilise supporters have been persecuted under the laws examined in the previous chapter. This section shows that they have been criminally prosecuted through provisions which are vague and arbitrarily interpreted by government officials.

Since the 2014 military coup, there has been a sharp increase in detentions and prosecutions under Article 112 (the lèse-majesté law) of the Penal Code to suppress undesirable opinions against the monarchy. Prosecutions under this provision were temporarily suspended from 2017 and throughout 2018, all 7 lèse-majesté cases prior to 2018 were dismissed by the court (iLaw, 2019c). However, use of the provision resumed when pro-democracy demonstrations escalated in 2020. The current wave of lèse-majesté charges was

announced by the Prime Minister Prayuth on 19 November 2020, who said that the government would enforce 'all laws and articles' against pro-democracy leaders and protesters. As of March 2022, Thai Lawyers for Human Rights (**TLHR**) reported that at least 183 people have been charged under Article 112 in 194 political cases (TLHR, 2022a).

According to iLaw, as of November 2021, most lèse-majeste prosecutions were related to online content. These include 68 cases relate to Facebook and Twitter posts; 51 cases are charges from public speaking; 23 cases from burning or bringing down portraits of the King; 19 cases from raising banners; and 8 people from wearing crop tops (habitually worn by the King during his time in Germany) (iLaw, 2021). Anchan Preelert, a 63-year old former revenue officer, was issued the most draconian sentence in recent years, (Freedom House, 2021) sentenced to more than 43 years in jail for sharing online posts criticising the royal family. Her sentence was halved from 87 years in prison after she confessed. Her case was first raised by the UN independent experts in 2016. In February 2021, the Special Rapporteur on the right to freedom of opinion and expression, the Working Group on Arbitrary Detention (**WGAD**), and the Special Rapporteur on the rights to peaceful assembly and of association issued a public statement urging the Court of Appeal to reconsider the case in line with international human rights standards and set aside the harsh sentence (OHCHR, 2021). Later in November 2021, the WGAD issued an opinion urging Thai authorities to immediately release Anchan. In their opinion, the WGAD also asked Thai authorities to consider the threat of the COVID-19 pandemic in detention places and to accord her an enforceable right to compensation and other reparations (TLHR, 2022b).

In addition, Article 116 (the sedition law) under the Penal Code has also been increasingly used by the military regime to shut down critics since the 2014 coup. iLaw, a non-profit organisation advocating for social reform, has noted that since the military coup in 2014 there has been a rise in prosecutions under Article 116, with claims ranging from criticising or talking about the coup or the NCPO, criticising the lèse-majesté law, the drafted constitution and rumours of counter-coup and national separatist movement (iLaw, 2017a). As of March 2022, TLHR reports that at least 125 people are charged under Article 116 in 39 cases that are related to politics (TLHR, 2021a).

Prosecutions under the sedition law cause three major political effects. First, this law, with a 7-year jail term, is utilised to threaten and create fear. Second, it imposes a financial burden on a defendant as it requires a large amount of money for bail. Third, it is used to legitimise the prosecution of pro-democracy protesters, since sedition is perceived as a very serious offence (iLaw, 2015). Between 2018–2019, when Section 112 (lèse-majesté) prosecutions were suspended, Section 116 was imposed as a substitute charge to prosecute those who express critical opinions against the monarchy (iLaw, 2019d). This practice ended with the policy reinstating the use of Section 112. A well-known prosecution under Section 116 was Pravit Rojanaphruk. A senior reporter at Khaosod English, he was charged in 2017 for violating Article 116 of the Penal Code over Facebook posts criticising the military regime (Prachatai, 2017).

The defamation laws have also been abused as tools to silence and punish government critics, activists and journalists (Bangkok Post, 2019). These provisions are also exploited by the private sector and the government in the form of SLAPPs and other judicial harassment against dissenting voices –

usually towards human rights defenders. For example, as of April 2020, Thammakaset, a chicken farm company, has brought 35 defamation lawsuits against 22 people over offline and online communications about alleged labour rights violations at Thammakaset farm (Prachatai, 2020). In July 2021, Prime Minister Prayuth took legal action against an 18 year old rapper, Danupa 'Milli' Kanaterrakul for posting tweets criticising Prayuth's handling of the COVID-19 situation (Sattaburuth, 2021).

The CCA is another legal tool that curtails internet freedoms. As of March 2022, TLHR reported that under the Act, 120 people were charged in 136 political cases (TLHR, 2021a). In 2018, the former Thammasat University rector Charnvit Kasetsiri was charged with violating the CCA for reposting a photograph of a handbag carried by Prime Minister Prayuth's wife on Facebook (Charuvastra, 2018a). Police stated in a complaint that the post committed an offence under Section 14 (2) and (5) causing the public to panic and damage to the country (iLaw, 2018). In 2020, a charge against Danai Usma, a graffiti artist from Phuket, was filed by the Airports of Thailand (**AOT**) under the Computer Crime Act for posting on Facebook criticising the COVID-19 screening measures at national Suvarnabhumi Airport. Later in 2021, the Court acquitted Danai's case, stating that Danai posted the text on Facebook without intention to cause public panic or disseminate false information (TLHR, 2022c). In 2015 Chiranuch Premchaiporn, the director of Prachatai, an independent non-profit online newspaper that covered underreported issues in Thailand, especially democratisation and human rights, was convicted by the Supreme Court under Article 15 of the CCA for failing to delete lèse-majesté comments on the Prachatai web forum. The Court also found that she did not fully cooperate with the authorities in deleting illegal content. The Court sentenced Chiranuch to eight months imprisonment and THB 20,000 (USD 589) fine with a jail term suspended for one year (Prachatai, 2015). As giant tech companies, in 2020, Facebook and Twitter faced legal actions under the CCA taken by MDES for the first time for allegedly ignoring requests to remove online content (Tanakasempipat and Thepgumpanat, 2020).

The Emergency Decree and its follow-up Orders and Announcements are issued to curb freedom of expression and media freedom in the digital space. In October 2020, the Commissioner General of the Royal Thai Police (as a Chief Official who is responsible for remedying the emergency situation) issued an Order no. 4/2020 requesting the NBTC and MDES to monitor and shut down four online media – Voice TV, Prachatai, the Reporters and the Standard – as well as Free Youth Facebook Page, a pro-democracy movement site. They were alleged to have violated the emergency decree, which prohibits disseminating information that causes unrest or affects good morals of the people. However, the Order was later overturned by the court. Based on Article 35 of the Constitution, the court ruled that the complainant did not specify which content or report of the media outlet was illegal. The court also stated that the law only permits blocking specific content, not an entire channel (Prachatai, 2020b).

The national laws and legislations contain vague language open to wide interpretation, impose severe punishments and give far-reaching powers to the authorities. They are enforced against internet users and curtail internet freedom. Although several cases were dismissed later by the court, prosecutions are carried out to silence dissenters and create an atmosphere of fear among people that leads to self-censorship.

3c. Rebukes, Harassment and Manipulation

Public rebukes, gender-based harassment and information operations (**IOs**) are additional tactics adopted by government and non-governmental actors in Thailand to suppress internet freedom and manipulate online narratives that are favourable to the military regime and unfavourable to political critics. These actions serve as psychological pressure to discourage political critics, independent journalists and human rights defenders, and deceive internet users.

Public rebukes are systematically adopted throughout the state apparatus and pro-government movements. In 2020, the Thai royalist activist and retired army captain Songklod 'Pukem' Chuenchoopo, together with a team of volunteers, created two Google Maps listing the names and addresses of nearly 500 pro-democracy activists allegedly opposing the monarchy. The 'witch hunt' map included personal information of pro-democracy activists, many of them students, together with their photos in university or high school uniforms. However, the maps were taken down later by social media companies for violating its policies (Potkin and Wongcha-um, 2021).

In April 2021, Prime Minister Prayuth threatened to bring legal action against internet users posting about the 'Thai Khu Fah Club'. The Government House (Thai Khu Fah Building) was mocked as a nightclub after the Minister for Transportation contracted COVID-19 at a nightclub in Thong Lor, Bangkok (Amarintv, 2021). In July 2021, MDES Minister Chaiwut Thanakamanusorn warned celebrities and online influencers not to use social media platforms to criticise the government and that such actions could be construed as disinformation (Khaosod, 2021), which is punishable by law. In response to the Minister's stance, the police conducted an investigation against more than 25 celebrities and influencers for allegedly criticising the government over its handling of the COVID-19 pandemic. Police also threatened that while freedom of expression is a basic right, it should be put under a legal framework (Bangkok Post, 2021b).

In Thailand's patriarchal society, women and lesbian, gay, bisexual and transexual persons (**LGBTs**) were especially isolated and became targets of gender-based harassment and intimidation by government-affiliated and non-governmental actors for their activities. Transgender activist Chitsanupong Nithiwana reported in 2021 that she faces online harassment in forms of transphobic comments questioning her sexuality (Prachatai, 2021). Between 2019–2020, women human rights defenders working on Deep South-related issues were specifically attacked on military-backed social media and websites. Angkhana Neelapaijit, Pornpen Khongkajornkiat and Anchana Heemena were among those targeted. They were constantly attacked and harassed on military backed websites and social media including *pulony.blogspot.com*. Sarinee Achavanuntakul, a social critic and well known writer, and Kunthida Rungruengkiat, a former deputy leader of now-outlawed opposition Future Forward Party were also listed in a 'watchlist' on various social media accounts. In 2020, Sirin Mungcharoen, a student activist at Chulalongkorn University, faced a storm of online sexual harassment after she posted content about feminism and gender equality on her social media accounts (Prachatai, 2020c). In 2018, a famous pro-democracy activist, Nuttaa Mahattana became a target of rape threat after voicing an opinion against death penalty for rapists (Charuvastra, 2018b).

A non-state actor, the poultry farm Thammakaset, has since 2018 brought legal actions against women human rights defenders, lecturers and reporters including Sutharee Wannasiri, Suchanee Cloitre, Ngamsuk Ruttanasatian, Angkhana Neelaphaijit, Puttanee Kangkun and Thanaporn Saleephol for their posting of information about labour rights abuses and encouraging fellow women human rights defenders.

IOs were extensively used as a tactic by the Thai Army during the anti-communist insurgency campaign in the 1960s–70s. Since 2006, IOs have been revamped for online utilisation in the context of the political conflicts and the insurgency in Southern Thailand (Sombatpoonsiri, 2022). In March 2021, Facebook removed 185 army-linked accounts including 77 accounts, 72 pages and 18 groups on Facebook and 18 accounts on Instagram. The platform stated that these accounts were linked to the Thai military's ISOC and targeted audiences in the Southern provinces of Thailand. Facebook also revealed that such action was based on coordinated inauthentic behaviour on the platform including posting content to promote the army and monarchy as well as criticising insurgent groups in southern Thailand (Tanakasempipat, 2021).

In October 2020, Twitter suspended 926 army-linked accounts amplifying pro-army and pro-government content as well as engaging in coordinated behaviour targeting prominent political opposition parties, namely the Future Forward Party (before the dissolution) and Move Forward Party. A study of the Stanford Internet Observatory (**SIO**), a cyber policy centre, found that information operations carried out by the Thai authorities are coordinated but ineffective and cause low impact because most of these accounts have no followers and the majority of tweets received no engagement. SIO also points out that Twitter has suspended a network of accounts linked to the Thai Army for the first time (Goldstein et. al, 2020).

3d. Defiance in the Face of Censorship

Self-censorship is a normalised practice of mainstream media in Thailand for business survival and to avoid being attacked by the government (Khaosod English, 2021). Critical portrayals of the monarchy and the military regime are considered taboo, while sensitive topics such as political scandals or environmental damages are regularly sidelined by mainstream media. The well-known scholar and political exile, Pavin Chachavalpongpun remarked that the leading media outlets, including ThaiRath and Daily News, never present any report that is deemed critical of the army or the monarchy (Chachavalpongpun, 2020).

In 2020, at the peak of the political demonstrations, mainstream media noticeably refrained from reporting about the pro-democracy movement and the excessive crackdowns executed by the government. Only online independent media outlets provide live-streamed, up-to-date, factual reportage. In 2021, self-censorship was further institutionalised by NBTC warning to the media not to broadcast the 10 political demands for monarchy reform put forward by the pro-democracy movement after the Constitutional Court ruled that such demands are an attempt to overthrow

Thailand's constitutional monarchy[9] (Prachatai, 2021b). As an another example, the Asian Human Rights Commission (**AHRC**) noted that in 2006, a case of a man arrested over painting over images of the Thai King had no coverage in Thai media (AHRC, 2006).

However, it must be noted that although a surveillance and censorship system has been established, Thai people have continued to resist and oppose the system. Several incidents proved that Thai people are defiant and show their resistance in the online space. In September 2012, a hacker posted messages in Thai and English on the Education Ministry's website that the ministry should have no right to control teenagers and called for freedoms and democracy. A student from a leading school later admitted that he was the hacker and told the Education Ministry permanent secretary Sasithara Phichaicharnnarong that he was upset by the Ministry's Jit Arsa (volunteering spirit) programme. The hacking caused the website to malfunction and the Ministry's IT and communications officials had to close the website down temporarily (Fredrickson, 2012).

In October 2015, an activist group, Thailand F5 Cyber Army, announced a 'cyber war against the authoritarian government' and called on the government to halt the single gateway proposal. The group repeatedly engaged in a distributed denial of service (**DDoS**) attack (rapidly and repeatedly accessing the server to overload it) (Wongsamuth, 2015).

A study of Shen and Tsui in 2016 showed that respondents in Thailand expressed moderate support for internet freedom and internet censorship. They found that in response to internet censorship, Thai netizens adopt various anti-censorship tools: 18.3% of Thais reported using a form of circumvention to access the censored content; 27.3% reported using an anonymisation tools to safeguard their identity; and 30.8% reported using messaging encryption apps to secure their email and instant messaging communication (Shen and Tsui, 2016).

In 2019, as some residents in parts of Southern Thailand were required by the Thai government to re-register their SIM cards, Asia Centre received a report that some local people managed to avoid the compulsory registration by struggling to use free wi-fi hotspots.

In 2020, when access was restricted to the Facebook group 'Royalist Marketplace' which gathered 1 million monarchy reformists, the group's founder Pavin Chachavalpongpun opened a new Facebook group 'Royalist Marketplace – Talad Luang'[10] on the same day. It garnered more than 375,000 members in only 5 hours. One day before the restriction, the MDES filed a police complaint against Pavin for being the admin of the original Royalist Marketplace, filing six offences against the Section 14 (3) of the CCA (Prachatai, 2020d).

In July 2021, information of the Bhum Jai Thai party, one of the government coalition parties, was edited on Wikipedia. The party was changed its name from Bhum Jai Thai (proud of Thai) to Bhum Jai Tu (proud of Tu (a nickname of PM Prayuth). Its motto was also changed to 'diminish people's power, increase cannabis's power [as the party was infamous in its policy of legalising Marijuana use], and lick dictator's boots' (Matichon, 2021).

[9] The regime is officially known as a 'democratic regime with the king as the head of state'.

[10] As of April 2022, Royalist Marketplace Talad Luang remains one of the 20 largest Facebook groups in the world and has over 2 million members.

In November 2021, Thailand's Constitutional Court website was hacked after issuing the decision that the pro-democracy leaders were attempting to overthrow the constitutional monarchy in August 2020. Its homepage was renamed to 'Kangaroo Court' and a YouTube video of the song 'Guillotine (It goes Yah)' by Death Grips was posted on the page (Thai PBS World, 2021).

National legislation that contains overbroad language for extensive interpretation and attach harsh punishments are enforced to limit internet freedoms. The measures have been intensified since the 2014 military coup. As a result, online content is blocked and removed; internet users are prosecuted; online harassment is widespread; and self-censorship is practised. Another issue to note is also the culture of impunity these laws.

Thai authorities consistently fail to investigate and prosecute attacks against journalists and citizen journalists who promote opposition views, protecting only state-owned media from public complaints and scrutiny. In addition, security authorities enjoy impunity for IO campaigns and attacks on journalists. Likewise, pro-royalist vigilante groups engaging in well-documented harassment and attacks on human rights defenders including journalist also enjoy freedom from prosecution (Destination Justice and Asia Centre, 2022). In the next section, key recommendations are presented for international organisations, technology companies and civil society to uphold internet freedom, lessen negative impacts, and create a more democratic environment in the digital space in Thailand.

4. Recommendations

Following a review of Thailand's existing legislation and its alignment with international human rights standards, it is evident that existing laws are utilised to curtail internet freedoms and fails to safeguard internet users especially in relation to freedom of expression, media freedom and the right to privacy. To uphold and safeguard internet freedoms, this section outlines a set of recommendations to advocate internet freedoms.

To the government of Thailand

- Amend Articles 34, 35 and 36 of the Constitution, eliminating vague and ambiguous language so that these Sections can be used to protect internet freedom appropriately.
- Amend exceptions to Articles 34, 35 and 36 of the Constitution to align them with international human rights standards considering principles of necessity, proportionality and non-discrimination.
- Explicitly specify guarantees of internet freedoms in the Constitution.
- Repeal or significantly amend Article 112 (lèse-majesté) and 116 (sedition) of the Penal Code that contain vague and ambiguous language open to arbitrary and extensive interpretation and which do not align with international human rights standards. These laws can be more appropriately placed in the Civil Code. Parliamentarians should play a leading role in amending Article 112 as they enjoy the legal protection of parliamentary privilege.
- Decriminalise defamation under Article 326, 327 and 328 of the Penal Code and situate it solely within the Civil Code.
- Enforce Article 161/1 and 165/2 of the Criminal Procedure Code entered into force to prevent SLAPPs.
- Amend Articles of the Computer Crime Act deleting vague and overbroad language open to arbitrary and extensive interpretation of the authorities, replacing them with clear wording, including intentionality requirement for commission and reducing the currently harsh penalties.
- Amend the Cybersecurity Act deleting vague and overbroad language open to wide interpretation and limit the extensive power of the authorities in establishing the digital surveillance system.
- Significantly amend the Emergency Decree so as to provide the judiciary and parliamentary bodies with powers to check the Executive. The terms of usage should also be strict, disallowing its use to limit political expression and mobilisation.
- Stop harassing and prosecuting individuals who exercise their internet freedom, refrain from putting pressure on tech companies in blocking and removing content, cease non-legal measures such as information operations against political dissenters and human rights defenders, and commit to international human rights standards.
- Comply with recommendations of member states and stakeholders during the UPR process and ICCPR review.
- Raise awareness that public figures, including those exercising the highest political authority and highest moral authority, are legitimately subject to criticism.

To the NHRCT

- Oversee the allegations of harassment, prosecution and other forms of human rights violation against internet users.
- Work closely with the government to comply with international human rights standards.

To tech companies

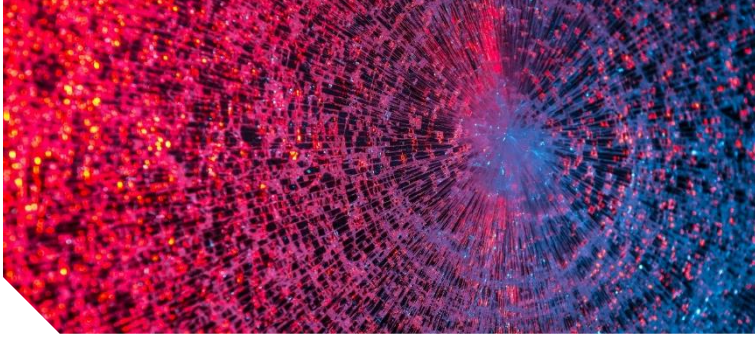
- Adhere to international human rights standards.
- Cooperate with CSOs.
- Publicise their detailed transparency reports enumerating all removing and blocking requests by the government.

To national, regional and international NGOs

- Continue documentation of harassment systematically.
- Provide risk assessment assistance to the human rights defenders and activists at risk.
- Engage national and UN human rights mechanisms.

To private sector companies

- Refrain from curtailing citizens' rights to free expression by frivolously exploiting such problematic laws, including through SLAPPs.



5. Conclusion

Internet freedoms are fundamental human rights in the digital age. Individuals must be able to access, use, create, and disseminate digital content or to access and use computers, mobile phones or other electronic devices and telecommunications networks. Internet freedoms are affirmed by international human rights mechanisms. Therefore, disconnecting people from the internet is a human rights violation and runs counter to international human rights standards.

In Thailand, the internet landscape is advantageous to internet freedoms. The internet penetration in the country has reached 70% of the total population and its infrastructure is also competitive. People have long exercised their internet freedoms and freedom of expression via online media platforms.

However, since the 2014 military coup, internet freedoms in Thailand have become under threat and are vulnerable. Several pieces of harsh legislation, including sections of the Penal Code, the CCA and the Cybersecurity Act, are enforced against individuals to curb undesirable opinions and expressions on the online space. In the backdrop of political demonstration and COVID-19 outbreak, internet freedoms violations in Thailand worsened when the Emergency Decree was issued in 2020. In addition, non-legal measures such as IOs and fake news crackdowns have been further adopted by the Thai authorities to attack dissidents in the online sphere.

Legal and non-legal measures adopted by the government have established the surveillance system, created an atmosphere of fear in the online space and caused negative impacts on internet freedoms. Tech companies are pressured to remove and block undesirable online content. Internet users who show hostile expressions and content against the monarchy and government are prosecuted with serious charges. Harassment against dissent is common. Online media and internet users practise self-censorship to survive and avoid being attacked.

However, the resilient Thai people oppose enforcement in nature. The strict surveillance system of the government will be challenged. In examining the strict legislation in place, this report recommends that legislators should ensure that the existing provisions are aligned with the international human rights standards and amend or repeal any law that does not comply with them. The Government should enforce existing legislation based on necessity, legality and proportionality, and avoid violating fundamental rights and freedoms of people.