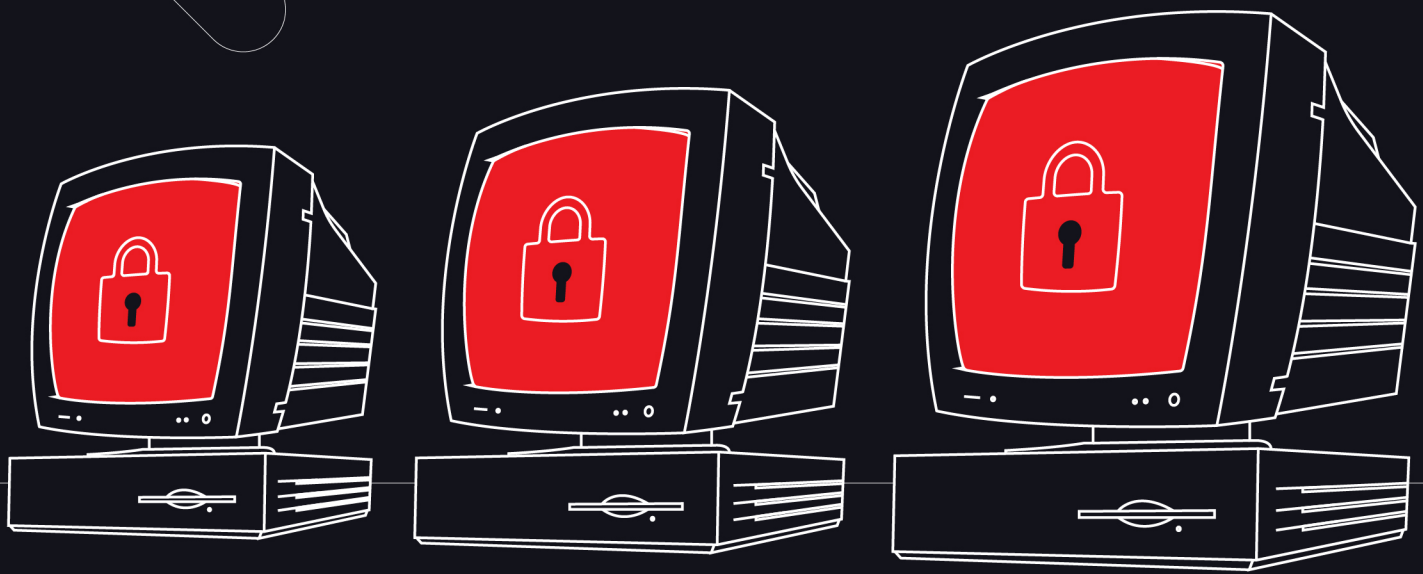
EngageMedia ASIACENTRE

Thailand Computer Crime Act

~~Restricting~~ Digital Rights, ~~Silencing~~ Online Critics



EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

Learn more at engagemedia.org.

Asia Centre is a research institute in Special Consultative Status with the United Nations' Economic and Social Council. The Centre undertakes evidence-based research, convenes events and amplifies its work through media and social media engagement in the area of freedom of expression and digital rights.

Learn more at asiacentre.org

Research:

Korbkusol Neelapaichit, Researcher, Asia Centre

Ekmongkhon Puridej, Research Assistant, Asia Centre

Advisory Team:

Yawee Butrkrawee, Digital Rights Manager (Mekong), EngageMedia

Dr James Gomez, Regional Director, Asia Centre

Egbert Wits, Research and Development Manager, EngageMedia

Editorial:

Katerina Francisco, Editorial Coordinator, EngageMedia

Special thanks to the following:

Alan Morrison, former Phuketwan journalist

Chiranuch Premchaiporn, former Director of Prachatai

Chutima Sidasathian, former Phuketwan journalist

Dechathorn Bamrungmuang, Rap Against Dictatorship (RAD)

Montana Duangprapa, Thai Lawyers for Human Rights (TLHR)

Orapin Yingyongpathana, former policy advocate

Dr. Pavin Chachavalpongpun, Associate Professor, Kyoto University

Poonsuk Poonsukchareon, Thai Lawyers for Human Rights (TLHR)

Dr. Piyabutr Bunaramrueang, Professor of Law, Chulalongkorn University

Thitirat Thipsamritkul, Professor of Law, Thammasat University

Yingcheep Atchanont, iLaw

Note: Some respondents have opted not to be identified in this study.

Published May 2022

Supported by the International Centre for Not-for-Profit Law (ICNL)

TABLE OF CONTENTS

Executive Summary **3**

Introduction **5**

1a. Background 5

1b. Adherance to International Law 8

The Computer Crime Act **10**

2a. Overview 10

2b. Key Sections 10

2c. Analysis 13

Impact **19**

3a. Denying access to critical content 19

3b. Harassment 22

3c. Prosecution 24

3d. Putting Pressure on ISPs and Tech Companies 27

Recommendations **32**

Bibliography **35**

EXECUTIVE SUMMARY

Before 2007, internet penetration in Thailand was low and the authorities had no law in place to tackle undesirable online content and criminalise internet offenders. As internet rates grew and online political expression became more prevalent, the Computer Crime Act (CCA) was introduced to plug the legal gap. In 2017, the Act was amended to strengthen its enforcement. Since its introduction in 2007, the CCA has been utilised to restrict digital rights and silence dissenters by prosecuting individuals and internet service providers (ISPs) while blocking websites or removing content.

This policy paper reviews the provisions of the CCA and aims to show why it is problematic. The Act contains vaguely-worded provisions subject to the extensive interpretation and discretion of the authorities, attaches harsh criminal penalties, and does not align with the International Covenant on Civil and Political Rights (ICCPR). The net result is that the CCA restricts digital rights, including freedom of expression and rights to privacy in Thailand.

Under its provisions, undesirable websites and content can be blocked or removed as directed by the court and authorities. Individuals or media expressing opinions against the establishment or monarchy can be prosecuted under the CCA. The Act has placed ISPs under pressure to balance compliance with court orders to block or remove URLs and the protection of users' fundamental rights. Often, the Act is exploited by the authorities to harass internet users and create an atmosphere of fear, leading to self-censorship.

In 2022, the Ministry of Digital Economy and Society (MDES) announced that the government is considering amending the CCA and studying the possibility of using a single

internet gateway to tackle overseas cyber criminals targeting Thai people, control the flow of illegal information online, and improve the safety of internet users. Based on past use of the law, however, these proposed amendments do not inspire confidence that online political expression would not be affected.

This policy paper recommends that the Thai government review and amend rights-infringing sections of the CCA, lessen harsh criminal penalties, promote digital literacy, and ensure that the provisions comply with international human rights standards. This Act and its enforcement needs to meet the measures of necessity, legality, and proportionality, and should not be used to block the flow of information and silence political critics.

I. INTRODUCTION

This policy paper reviews key provisions of the CCA, shows why the Act is problematic, and discusses the impact of this law on digital rights. Key recommendations to promote and protect digital rights in Thailand are presented as a conclusion. This paper incorporates desk research and online consultations undertaken from 21 February to 12 April 2022. Documents reviewed include both primary and secondary sources such as United Nations documents, the CCA (2007) and its Amendment (2017), as well as other relevant reports from media and international nongovernmental organisations (INGOs) on the application of the CCA. A total of 15 online consultations with academics, civil society activists, human rights lawyers, representatives from the technology sector, and policy advocates were conducted to gather views and experiences and validate the desk research.

1a. Background

The CCA took effect on 18 July 2007 after the adoption by the National Legislative Assembly (NLA) appointed by the Council for National Security (CNS). Before the CCA was enacted, there was no specific legal tool for Thai authorities to tackle issues of internet

crimes and online harmful content.[1] When it was introduced, internet users in Thailand comprised 20.03% of the total population of 66 million.[2]

Following the enactment, the Act's vague provisions and exploitative use were primarily targeted towards political activists and became a source of great concern both inside and outside the country. Thai authorities issued orders to block or remove politically-critical content and, using the CCA, prosecuted dissenters. Prosecutions under the Act were on an upward trend from July 2007 to July 2010. During the three years of enforcement, there were a total of 185 cases: 9 cases in 2007, 28 cases in 2008, 72 cases in 2009, and 76 cases in 2010.[3]

Following the July 2011 general election, Pheu Thai Party captured a clear majority in parliament and Yingluck Shinawatra became the Prime Minister. In October 2011, her official twitter account @PouYingluck was reportedly hacked, posting 8 messages criticising Pheu Thai's policies and accusing the party of cronyism and nepotism. The Ministry of Information Communication Technology (ICT) revealed that the hacker, a university student, was arrested for breaking Section 7 of the CCA and faced up to two years in prison and a fine of no more than THB 40,000 (USD 1,177).[4]

The Yingluck government was targeted by the People's Democratic Reform Committee (PDRC) with widespread protests, eventually leading to a military coup in 2014. Under the military government of Prayuth Chan-o-cha, plans were put into motion to amend the CCA in 2016 by the military-backed NLA on the official pretext of upgrading the law to tackle complex internet offences and protecting national cybersecurity. However, iLaw (2016) argued that the existing law provided insufficient power for the authorities in prosecuting those who committed online offences and to control harmful content.[5]

---

1 Tunsarawuth and Mendel (2010)

2 ITU (2020) and World Bank (2020)

3 Sawatree, Kusonsinwut, and Yingyongpathana, (2010)

4 Thairath Online (2011)

5 iLaw (2016a)

The move to amend the CCA faced online and offline protests from activists and netizens.[6] In the online space, Thai Netizen Network hosted a petition on *Change.org* calling on the NLA to reject the amendment, attracting more than 350,000 signatures of support.[7] By 2017, as internet penetration in the country had gone up to nearly 53%, Prime Minister Prayuth insisted that the Amendment was necessary for the government to increase its ability to remove 'undesirable online content'. [8, 9] The Amendment to the CCA came into force on 24 May 2017.

The Act continues to be criticised for its abusive use to restrict digital rights and silence political dissent. The Court of Justice[10] (2022) revealed that since the 2014 military coup, the number of offences under the CCA has significantly increased as shown in Table 1.

Table 1: Number of CCA offences from 2013-2019

Year	2013	2014	2015	2016	2017	2018	2019 (Jan - Sep)[11]
No. of CCA offences	86	125	451	874	886	978	823

Source: The Court of Justice (2022)

Updated information from We Are Social and KEPIOS shows that in 2022, internet users in Thailand rose to 77% of the total 70 million population. Meanwhile, social media users in the country comprised 81% of the total population.[12] Between 2020-2022, the internet landscape was marked by political protests led by youth and students calling for democracy and monarchy reform. The internet and social media have been widely used to disseminate their ideologies, mobilise supporters, and fight back against the government.

6 Nanum (2016)
7 Change.org (2016)
8 Undesirable content in the policy paper means content that presents a negative attitude towards the government and monarchy.
9 Reuters (2016)
10 The Court of Justice (2020)
11 This is the latest information from the Court of Justice that is publicly available.
12 We Are Social and KEPIOS (2022)

However, in 2022, the Ministry of Digital Economy and Society revealed that the government is considering amending the CCA and studying the possibility of using a single internet gateway. Its intended aim is to address the problem of overseas cyber criminals targeting Thai people; control the flow of illegal information online; and improve the safety of internet users.[13]

1b. Adherence to International Law

Thailand's adherence to international human rights standards can be assessed by its compliance with the International Covenant on Civil and Political Rights (ICCPR) and Universal Periodic Review (UPR).

As a state party, Thailand has been slow to submit its ICCPR state party reports. It submitted a report for the 1998 cycle in 2004 and for the 2009 cycle in 2015. In the 2015 state party report, the government argued that the CCA was enacted so that the authorities can more effectively deal with a range of criminal and harmful activities committed via computers and the internet. [14] However, in the concluding observations of the Human Rights Committee of the ICCPR dated 25 April 2017, the Committee expressed concern over restrictions imposed on the right to freedom of opinion and expression in multiple national laws, and particularly in the CCA (2007). It recommended that Thailand should refrain from using its criminal provisions, including the CCA, as tools to suppress the expression of critical and dissenting opinion.[15]

Thailand has participated in the UPR processes in the 2011, 2016 and 2021 cycles. Issues related to the CCA have been raised across these cycles. During the first and third UPR cycles, the Special Rapporteur on the right to freedom of expression and the Human Rights Committee raised concerns over restrictions to the right to freedom of opinion and expression in Thailand, mainly through laws such as the CCA.[16] The CCA was attacked for its inconsistency with international human rights standards and vague provisions.[17] Meanwhile,

14 UNHRC (2015)

15 UNHRC (2017)

16 UNHRC, 2011a and; UNHRC, 2021a

17 UNHRC, 2021b

stakeholders observed the authorities' increased use of legislation to silence peaceful political dissent.[18] In the first and third UPR processes, the well-known case of Chiranuch Premchaiporn was cited. Premchaiporn, the female director of Prachatai – an independent online media covering underreported issues in Thailand, especially about democratisation and human rights – was charged under the CCA for not removing online anti-monarchy comments from the website. During the UPR cycles, parties recommended that the Thai Government cease prosecutions under the CCA and amend or repeal the Act.

There is no international standard on cybercrime legislation. The 2001 Council of Europe Convention on Cybercrime provides the most relevant and useful model for developing a cybercrime law. The convention includes chapters of definitions, offences, international cooperation, and final provisions. Importantly, it ensures balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the ICCPR. [19] However, Thailand is not a state party to this Convention.

18 UNHRC, 2011b

19 Convention on Cybercrime, 2001

II.
THE COMPUTER CRIME ACT

This section reviews the key provisions of the 2007 CCA and its Amendment to explore what remained and changed in the law. It also expounds on reasons why the CCA is and remains problematic.

2a. Overview

The CCA carries a total of 31 provisions and can be divided into three major parts: general provisions (Sections 1-4), online offences (Sections 5-17), and officials (Sections 18-31). Online offences can be separated into two main groups: offences against computer systems or computer data (Sections 5-13, covering illegal access to computer data or systems, disclosure of security measures, unauthorised interception and interference, and spam) and content offences committed via computer (Sections 14-16).

2b. Key Sections

This paper will focus on reviewing Sections 14, 15, 18, 20, and 26 of the Act because these sections have become contentious for their restriction of digital rights by criminalising internet users and ISPs, giving far-reaching power to the authorities during investigations,

Section 14: In the 2007 Act, Section 14 imposed up to five years of imprisonment or a fine of up to THB 100,000 (USD 2,972) or both, for entering forged data into a computer that is deemed to cause damage to a third party or the public, (1) or to national security or to cause public panic (2); inputting data which is an offence relating to the security of the Kingdom or terrorism offence under the Penal Code (3); or inputting pornographic data (4). This provision also includes the crime of disseminating or forwarding the above mentioned data (sub-section 5).

In the 2017 Act, Section 14 added restrictions to the use of the CCA by requiring ill or fraudulent intent for committing an offence and covered the entry of distorted data into a computer. It also excluded defamation under the Penal Code. However, it added the entry of false computer data that is likely to damage the maintenance of national security, public safety, economic safety, or public infrastructure serving the nation's public interest.

Section 15: In the 2007 Act, this section criminalised service providers who 'intentionally' consent to or support the perpetration of the offences under Section 14 by using a computer system under their control. It imposes the same penalties as the offender under Section 14.

In the 2017 Amendment, the intention of committing an offence was removed as a requirement and expanded to cover ISPs who cooperate in the perpetration of the offences. Section 15 of the Amendment further directs the Minister for Digital Economy and Society to issue a notification specifying the process of issuing a warning, blocking the dissemination, and removing data from computer systems (notice and takedown mechanism). A service provider proving their compliance to the notification within a specified time frame will be exempted from penalty.

Section 18: In the 2007 Act, this section authorised officials to request statements from those related to the perpetration of an offence (1); to request traffic data from service providers (2); to order service providers to submit information relating to their clients (3); to duplicate data from computers suspected of being used for an offence (4); to order the computer data processor, controller, or those who own storage devices to deliver such data or devices (5); to inspect or access the computer system or storage device of anyone that is

evidence of the offence (6); to decode computer data of anyone (7); and to seize or attach any computer system for the purposes of investigation and evidence-gathering (8).

The 2017 Amendment provides that those who received the request from officials related to sub-sections (1), (2), and (3) shall act without delay as requested, but not longer than seven days since the request was received; or act within the time specified by officials.

A service provider who fails to comply with Section 18 shall be subject to a fine not exceeding THB 200,000 (USD 5,944) and a further daily fine not exceeding THB 5,000 (USD 148) per day until the relevant corrective action has been taken.

The 2017 Amendment also allowed inquiry officials as specified by the Criminal Procedure Code to ask any person empowered by the CCA to collect evidence of a criminal offence committed via a computer system or storage device. Similarly, if a criminal offence is uncovered as a result of an official's execution of duties per the CCA, the official shall urgently compile facts and evidence and inform the relevant authorities for further action.

Section 20: In the 2007 Act, this section allowed, with approval of the Minister, officials to apply for a court order to block the dissemination of any data that fell under the offences specified in the Act, or that was deemed to compromise the security of the Kingdom, relates to other criminal laws, or breaks the public order or good morals. After receiving the court order, the official may conduct the blocking himself/herself, or order the service provider to do so.

In the 2017 amendment, the Computer Data Screening Committee was established. The Minister, with the approval of the committee, may authorise officials to request a court order to suppress the dissemination or to remove computer data deemed contrary to the public order or good moral of the people.

Anyone who fails to comply with the court order or officials under Section 20 shall be subject to a fine not exceeding THB 200,000 (USD 5,944) and a further daily fine not exceeding THB 5,000 (USD 148) per day until the relevant corrective action has been taken.

Section 26: In the 2007 Act, this section requires service providers to retain traffic data for at least 90 days from the date on which the data was input into computer systems. If necessary, authorities may order the service provider to keep such data for a period longer than 90 days but not more than one year.

In the 2017 CCA, the service provider may be obliged to keep such data for longer than 90 days but not more than two years – an increase from the one-year limit in the 2007 CCA.

2c. Analysis

By reviewing the Act and undertaking consultations with key informants, this policy paper analyses the changes in the CCA and why it still proves to be problematic:

What remained

First, the CCA became a favoured 'magic wand' used by authoritarian regimes to silence critics and manipulate online narratives, in effect legitimating desirable opinions toward the establishment. As mentioned above, the Act was introduced by the CNS-backed government to plug the legal gap, then amended by the NCPO to upgrade the law, and was the subject for a second amendment initiated by the government of retired general Prayuth. In 2022, former prime minister Anand Panyarachun highlighted this pattern: that junta governments installed after coups had a tendency to misuse power or abuse the legal system to persecute people who hold different opinions.[20]

Second, instead of protecting digital rights, the CCA is a huge burden on internet users, intermediaries, and service providers. This law caused ordinary internet users to self-censor their posts, shares, following activity, or other online activities to avoid being punished or caught up into trouble. The CCA has placed a huge burden on those who were prosecuted, although their cases were eventually dismissed or suspended. The Act also imposed several liabilities on service providers. For example, under the CCA, service providers are required to

20 Bangkok Post, 2022b

take down undesirable data (Section 15), retain log files (Section 26), surrender such data to officials as requested (Section 18), and restrict access to websites as directed by a court order (Section 20). These burdens came at the expense of customer service improvement, product innovation, and eventually the creative economy.

Third, the CCA went against the nature of the internet which is decentralised, borderless, global, and ubiquitous. Considering the diversity of opinions online and the flow of big data through the internet, this law attempted to manipulate online narratives and control content. Furthermore, as the internet is borderless and worldwide, the CCA's attempt to block content access resulted in geoblocking or access restrictions only in Thailand.

What changed

First, control over CCA execution was changed. The execution of the 2007 CCA was under the Minister of ICT while the amended 2017 CCA is under the control of the Minister of MDES.

Second, the use of Section 14 (1) to penalise defamation was eliminated. After the 2007 CCA was introduced, most of the CCA prosecutions brought to the court were based on this section. Section 14 (1) of the 2007 CCA was strongly criticised by several sectors calling for its amendment because it overlapped with some provisions in the Penal Code, imposed harsh penalties, was not compromisable, lacked guarantee of good faith or public benefit, and eroded media freedom.[21] As shown in Chapter 3, the military agencies brought legal cases against human rights defenders and journalists.

Third, the Amendment increased pressure on ISPs. Section 15 criminalises service providers which cooperate, consent to, or support the perpetration of the offences under the Act, even without the need to establish intention of service providers. Under the Amendment, the Ministerial Notification also introduces the notice and takedown mechanism, exempting ISPs from punishment only if they take down content within a specific timeframe.

21 iLaw, 2014

Fourth, the Amendment introduced more vague words that are subject to broad and arbitrary interpretation by the authorities. For instance, Section 14 adds the words 'distorted' without a clear definition. In addition, notions of 'damages' to national security, public safety, or economic safety have been added to this provision, once again without specification.

Fifth, the Amendment increased penalties. Section 16 of the 2007 CCA imposed up to three years of imprisonment and/or a fine of no more than THB 60,000 (USD 1,783) on whoever enters a picture of another person into a computer system that causes defamation. In the 2017 Act, the fine was increased up to THB 200,000 (USD 5,944) with compulsory imprisonment of up to three years.

How the CCA is problematic:

First, as mentioned, the CCA contains vague and overbroad words without clear definitions. Section 14 (2), for example, specifies offences causing damage to national security, public safety, or economic safety, but does not provide clear definitions. As a result, this provision is subject to the broad and arbitrary interpretations by the authorities. An example was a case in Chiang Mai where an editor of a local lifestyle magazine faced criminal charges brought by the governor for allegedly breaking the CCA. This action came in 2018 after the editor shared on Facebook a photo depicting three iconic ancient kings wearing face masks to promote an anti-air pollution rally.

Second, the Act continues to give sweeping powers to officials, who are appointed by the Minister, without transparent procedures and judicial scrutiny for their use of power. For example, subsections (1), (2) and (3) of Section 18 gives officials investigating power to demand testimony or explanation from anyone related to an offence; request traffic data from service providers; and instruct service providers to surrender user-related data without the need for a warrant, any court supervision, or order.

Third, the CCA covers extensive categories of ISPs. Based on a definition and the 2021 Notification issued by the MDES, ISPs that will be regulated and liable under the Act broadly include telecommunication and broadcast carriers, access service providers, hosting

service providers, internet shop owners, online application stores, social media service providers, content and application service providers, cloud computing service providers, and digital service providers. This Act fails to distinguish between the different types of ISPs. For example, some ISPs only provide technical access without hosting or even having access to the content used by their clients.[22] Therefore, the Act's liability provisions sweepingly cover everyone facilitating internet or online services for others – ranging from broadband internet providers, mobile internet providers, internet cafes, companies, restaurants, and malls providing internet for customers or employees.[23] A representative from DTAC, one of Thailand's three major mobile phone service providers, noted in a 2016 seminar that Section 15 has affected mobile phone service providers. The companies, which worked as a 'pipe' carrying data to and from the internet, were held responsible for content that they did not create.[24]

Fourth, the CCA does not provide a mechanism for protecting privacy. No guarantee is provided on how traffic data kept by ISPs or accessed by the officials will be used or scoped. Section 18 allows officials to collect evidence of other criminal offences committed via a computer system and submitted to inquiry officials as specified in the Criminal Procedure Code for further action. This provision leaves room for violating rights to privacy. Montana Duangprapa and Poonsuk Poonsukchareon, two representatives from the Thai Lawyers for Human Rights (TLHR),[25] explained: "Under the CCA, officials may have a search warrant or consent to examine the accused's mobile phone. A mobile phone contains enormous data, including financial or personal information. The CCA does not guarantee how data that is accessed by the officials will be used or scoped. As a result, an investigation into a mobile phone can be magnified to encompass other criminal offences. An [example is the] interesting case of Burin Intin. He was arrested for illegal assembly in 2016. The authorities received consent from him to examine his mobile phone. Based on evidence collected from his phone, Intin was additionally charged for breaking the lèse-majesté law and the CCA. The authorities further found that his chat with Patnaree Chankij, mother of a famous student

22 Tunsarawuth and Mendel, 2010

23 Prachachat, 2019

24 iLaw, 2016b

25 A local organisation working to raise awareness about human rights violations and provide free legal support to people whose rights have been violated.

activist, was deemed to have broken the lèse-majesté law. So she was later charged with the law".[26]

Furthermore, the CCA allowed authorities to request data from service providers for investigation purposes and instruct these providers to submit user data that they were required to keep. The Act only requires ISPs to keep traffic data or log files within a specified time, but does not provide a mechanism for protecting user data. Information requests by the authorities also do not require any judicial authorisation.

Fifth, some offences under the Act overlap with offences under the Penal Code. Therefore, the CCA has been abused to increase punishment or impose harsher penalties against offenders. For example, Section 14 is used to prosecute those expressing critical opinions towards the monarchy via the internet, justifying through its sub-sections (2) or (3) supplementary harsher punishments provided under Section 112 of the Penal Code (lèse-majesté).[27] In one case, Section 14 of the CCA was used along with the sedition law to criminalise those criticising the government. In 2017, Pravit Rojanaphruk, a senior staff writer at the newspaper Khaosod English, was charged by the Technology Crime Suppression Division under the sedition law (Section 116 of the Penal Code) and Section 14 (3) of the CCA for his two Facebook posts criticising the draft charter of the Constitution and General Prayuth.

Sixth, there is a lack of public awareness on the implications of the CCA. The problem is a bit different from what has been mentioned above, but it is noteworthy because people's legal awareness is key to implementing the law and to prevent misuse by authorities. This issue was raised by Alan Morrison and Chutima Sidasathian, two former journalists from Phuketwan[28]: "Right now we are helping local people in Korat (the province of Nakhon Ratchasima). Farmers have allegedly been defrauded of as much as 100 million baht by officials. The main accused officer threatened to use the CCA to prosecute the villagers if they posted or shared any relevant comments about this crime. His action was designed to

26 Interview with Asia Centre on 16 March 2022

27 Tunsarawuth and Mendel, 2010

28 The Phuket-based news website that was prosecuted under the CCA.

silence people. Villagers feel scared because they have little knowledge of the provisions of the CCA and their own rights. It is important to educate everyone. We cannot avoid the CCA because so many people across Thailand use the internet every day. But citizens are mostly unaware of what they are entitled to say. They do not know how seriously the CCA violates their fundamental rights. The Act is used to limit freedom of expression and opinion."[29]

29 Interviewed with Asia Centre on 11 March 2022.

III. IMPACT

This section examines how the Act has impacted digital rights and freedom of expression online in Thailand.

3a. Denying access to critical content

The CCA allows the Thai government to compel technology companies to block and remove online content. The process for doing so begins with the MDES first submitting a request to the court to issue a takedown order. Upon issuance of the court order, the relevant authorities will either block access or remove the indicated content themselves, or order ISPs to comply by sending the court order to the National Broadcasting and Telecommunications Commission (NBTC), which will then instruct ISPs.

Under the 2007 CCA, most of the targeted content and sites were related to criticism against the government and monarchy as well as political mobilisations. In 2009, the ICT reportedly blocked 2,300 websites for allegedly insulting the monarchy.[30] After the 2017 Amendment, the Computer Data Screening Committee was introduced. This committee has authority to empower the Ministry to permit officials to request a court order for the

30 Southeast Asian Press Alliance, 2009

blocking or removal of any data which is contrary to the public orders or good morals of the Thai people. However, Dr. Piyabutr Bunaramrueang, a Professor of Law at Chulalongkorn University, commented: "In practice, the screening process had not been very effective. There is no significant implementation so far. The officials inevitably continue to petition for a court order to block or remove content."[31]. In 2020, three years after the CCA amendment, the MDES revealed that courts had issued orders to block 13,505 URLs that committed the lèse-majesté offences. Of these, 7,990 URLs were on Facebook. 3,058 URLs were on YouTube. 1,070 URLs were on Twitter, and 1,387 URLs were on other websites.[32]

In 2022, Google revealed that, since 2011, it received a total of 1,147 requests from the Thai authorities to remove content, of which 95.2% related to government criticism.[33] For YouTube, 64,686 videos were removed between October to December 2021 alone. Previously in July to September 2021, 163,800 videos were removed from the platform at the request of the Thai government.[34]

One such example was a music video titled 'Reform' by the Rap Against Dictatorship (RAD) band, which was blocked in early 2021 by YouTube after its release in November 2020. The song was created to connect with the protest of the 'Free Youth' calling for the monarchy reform. Dechathorn Bamrungmuang, a member of RAD, said: "Our band found the URL of the music video was inaccessible without any notification from the authorities. After we appealed to YouTube to unblock the URL, we received a reply that YouTube was requested by the Thai government to block the content immediately. To unblock this video, we needed to make a court appeal. As of April 2022, the request to unblock was still pending in the court. However, RAD re-uploaded the song 'Reform' again a few months after blocking, attracting nearly 12 million viewers as of updated data."[35]

From January 2012 to June 2021, Twitter received 191 demands from the Thai government to remove or withhold content. Total compliance rate of removal actions from Twitter is at

31 Interview with Asia Centre on 17 March 2022.

32 Posttoday, 2020

33 Leesa-Nguansuk, 2022

34 Google, 2021

35 Interview with Asia Centre on 6 March 2022.

12.1%.[36] Between January to June 2021, Facebook restricted access to 788 content pieces in Thailand as requested by the MDES for allegedly violating the lèse-majesté law.[37] On 24 August 2020, a notable Facebook group 'Royalist Marketplace', an online forum sharing content criticising the monarchy, was shut down and made inaccessible in Thailand. Group administrator Pavin Chachavalpongpun[38] was found guilty of six counts of breaking Section 14 (3) of the CCA.[39] However, on the same day, Pavin opened a new group called 'Royalist Marketplace – Talad Luang', attracting more than 2.4 million members as of March 2022.

Pavin, one of the founders of 112 Watch – a coalition of people and organisations aiming to halt the use of lèse-majesté law in Thailand – said: "When our group reached 1 million members, the government decided to take action against us. They move[d] to close our group. In the first step, the authorities threatened to use the CCA against me. When the threat failed, [they] moved to request the platform to close my group – a request which went against Facebook's community guidelines. They finally managed to request a geo-block of the group (limiting people in Thailand from accessing) with a threat of prosecution and daily fines should Facebook not comply."[40]

A technology company representative explained the removal request: "Online platforms received legal requests from the government to restrict content. But we did not remove the content. That was geo block. It meant anyone who tried to access the content in Thailand was not able to. If you accessed it from outside or [by] using VPN [virtual private networks], you were able to see the content."[41] This issue clearly reflects how the CCA goes against the nature of the internet which is decentralised, borderless, and worldwide.

The tech company and TLHR both point to the case of Thanathorn Juangroongruangkit, a political activist and the former leader of the disbanded Future Forward Party. In January 2021, a 30-minute video of Thanathorn criticising the royal COVID-19 vaccine program was

---

36 Twitter, 2021

37 Facebook, 2021

38 A well-known scholar, associate professor and political exile

39 Prachatai, 2020a

40 Interview with Asia Centre on 12 April 2022.

41 Interview with Asia Centre on 28 March 2022

blocked after the MDES requested a court order under Section 20 of the CCA. Thanathorn filed a petition against the restriction order. The Criminal Court called the MDES and Thanathorn to join re-inquiry and later revoked the blocking order, citing the protection of freedom of opinion under the Constitution and international standards. The two interviewees highlighted that prior to Thanathorn's case, the restriction orders by the court had always proceeded without a hearing nor allowing individuals to defend themselves. The case of Thanathorn set a new standard for considering blocking websites under Section 20 of the CCA, providing an opportunity for the URL/website owners to defend themselves and provide their evidence.

Media outlets also face similar challenges. In 2020, all online platforms of Voice TV, a local media outlet, were suspended for allegedly breaking the Emergency Decree and Section 14 of the CCA because they uploaded alleged false information into computer systems at the height of political protests in 2020.[42] In response, Voice TV issued a statement defending their position, saying that they did not spread misinformation or damage national security or public peace and order. The media outlet also stated that they have always adhered to democratic principles and will continue to produce news to serve society.[43]

3b. Harassment

Threats of using the CCA is another approach taken to curtail free expression in Thailand. In November 2017, Prime Minister Prayut threatened to 'rigorously' enforce the CCA on online media that distort facts and disseminate fake reports and hate speech.[44]

In 2017, MDES issued a notification requesting all citizens not to follow, contact, share, or engage in any activity that disseminated the content of historian Somsak Jeamteerasakul, Pavin, and online journalist Andrew MacGregor Marshall. The notification said that people who spread such information, directly or indirectly, could be violating the CCA, even unintentionally.[45]

---

42 Prachatai, 2020b

43 ibid

44 Sabpaitoon, 2017

45 Bangkok Post, 2017

Reflecting on this case, TLHR (2017) noted that this notification was just a communication, not an enforceable regulation. Limiting the rights and freedoms of people to follow, contact, share, or engage with these three persons is not allowed,[46] yet the threat of prosecution was enough to cause fear among netizens. Commenting on the notification, Pavin said: "It was an attempt to make me an online *persona non grata* and [deterred] people on Facebook from contacting me. In a positive way, I was better known by people. My social media followers increased immediately. Before that, I had around 200,000-300,000 followers. Nowadays I have almost 1 million followers. The notification caused counter productive impacts for the government. The government wanted to threaten netizens and reduce the number of my followers. Anyway, there was a little negative impact. A few people unfriended me because they felt fear. They did not want to have trouble. A few friends also unfriended me because their work could be affected. I felt disappointed and annoyed."

In 2018, Deputy Police Chief Pol. General Srivara Ransibrahmanakul threatened to file charges against RAD for allegedly violating the NCPO orders, the CCA, and the sedition laws. This was in response to the band's music video 'My Country's Got' ('Prathet Ku Mee'), which received close to 20 million viewers at the time on YouTube. The video touched upon and criticised several serious social and political issues in Thailand, such as the historic massacre, political polarisation, corruption, and military intervention in politics and law enforcement. In response, the Technology Crime Suppression Division stated that the music video may be considered an offence under Section 14 (2) of the CCA by entering online false information that is likely to damage national security. Those who shared or disseminated the video may be liable under Section 14 (5) of the Act.[47] Due to the fierce criticism by netizens, Pol. General Srivara later backtracked and confirmed that people can sing, listen to, and share the controversial song.[48]

Dechathorn, a member of RAD, said: "The song 'Prathet Ku Mee' was not blocked, but police threatened to use the CCA. And there was news that sharing the song would be illegal. The CCA was used to create fear and as a weapon of the regime to prosecute those who post

46 TLHR 2017

47 iLaw, 2018

48 The Nation, 2018

or share content. If used correctly, the CCA can tackle fake news or Information Operations or block gambling websites. Instead, the CCA was exploited by the authorities to silence internet users."

The use of the CCA has also been abused because it allows an incident to be reported to the police from any jurisdiction. Yingcheep Atchanont, a representative from iLaw, said: "The CCA has been used to persecute. The case of Suraphan Rujichaiwat can be [cited as an example]. In 2015, Suraphan, an environmental and anti-mining activist in the province of Loei, was prosecuted by a mining company for defamation and [for violating] the CCA Section 14 (1). The company said that Suraphan's message posted on Facebook was deemed defamatory and possibly led to mistrust among the company's customers as well as the public. Suraphan's case was filed with the Provincial Court of Mae Sot, the northern part of Thailand. Prior to this case, Suraphan had been prosecuted by the company for many [other cases]. One of these complaints was filed with the Provincial Court of Phuket in the southern part of the country."[49] This strategy has been adopted to silence and harass victims and enhance the burden on them. Chiranuch Premchaiporn, a media expert and advocate, further emphasised: "The CCA allowed a complainant to notify police from everywhere. Regardless of whether being proven guilty or not, it created a burden [on victims] from the beginning."[50]

3c. Prosecution

Since the 2014 military coup, prosecutions under the CCA have continued to increase. This section will present some notable cases showing how the CCA is and can be abused as a blanket tool to criminalise individuals and erode digital rights. Since the political demonstration broke out in 2020, 129 people have been charged under the CCA in 148 political cases as of April 2022, according to the TLHR.[51]

In 2009, immediately after the transitory provision of the CCA was finished, Chiranuch Premchaiporn, the director of Prachatai.com was charged under the CCA for failing to delete

49 Interview with Asia Centre, 11 March 2022.

50 Interview with Asia Centre, 25 March 2022.

51 TLHR, 2022

lèse-majesté comments on the Prachatai online forum. Later in 2010, she was charged under the CCA again for not deleting similar comments on the Prachatai news website. Speaking about this experience, Chiranuch stated: "Being prosecuted was not beyond my expectations. Because at that time, there was a small number of online media, and Prachatai provided space for expressing opinion and criticism against the dictatorship or authoritarianism. Being arrested at the first time was annoying, but not bad. I was prepared. It worsened in the second arrest because the first lawsuit remained pending and I was taken far to the police in northeast Khon Kaen province, where the case was brought. Legislation like the CCA was an approach that governments across the world [use in an attempt] to control and regulate the internet via [an] intermediary."

In 2015, Chiranuch was convicted by the Supreme Court under Section 15 of the CCA. The Court stated that Chiranuch did not fully cooperate with the authorities in deleting illegal content. The Court sentenced her to eight months imprisonment and THB 20,000 (USD 594) fine with a jail term suspended for one year.[52] The case of Chiranuch was under the spotlight of the international community and media advocates, putting pressure on the government. It was also highlighted during the first and third UPR cycles of Thailand.

In 2014, two former Phuketwan journalists, Chutima Sidasathian and Alan Morrison, were prosecuted for criminal defamation and violations of the CCA (Section 14). The case was brought forth by the Thai Royal Navy, which accused the two of publishing an excerpt of Reuters' investigation saying that the naval forces received benefits from the fleeing of Rohingya people. In 2015, the journalists were acquitted by the Phuket Provincial Court. Morrison said of the case: "At the time, it amazed me that reporting honestly about human trafficking brought that kind of reaction. I have worked in many countries. Nobody in those other countries would ever use charges of this kind against the media in that way. Phuketwan was affected terribly in the long term. After being prosecuted by the Navy, we lost potential advertisers because they did not want to have a problem with the Navy. It was a difficult battle. We decided to fight the case and keep Phuketwan going but in the end, even after our victory in court, we had to close."

52 Prachatai, 2015

Chutima further elaborated: "This was very tough. We lost so much time. We lost the energy to report essential information for the public. Phuketwan only wanted to put Thailand on the right path, to end the corruption, and to end the inhuman trafficking that caused Thailand's reputation to be damaged. The unfair charges even affected family relations. Alan's father was sick, but he was not able to fly home to see him. His father died without Alan being there. We lost the time to care for the people we loved. We spent all our energy running around and defending ourselves from this crazy thing. The authorities just tried to threaten/intimidate Phuketwan, using bad laws. This was very painful. It cost us a lot in many ways and I cannot estimate the price."

In 2016, the Internal Security Operations Command (ISOC) Region 4 Forward Command, which was established to resolve the situation in the deep South of Thailand, filed complaints against three human rights defenders – Pornpen Khongkachonkiet, Somchai Homlaor, and Anchana Heemmina – for breaking the defamation law and Section 14 (1) of the CCA. This stemmed from the three human rights defenders' work to publicise a report on the alleged torture and ill-treatment by Thai security forces in the deep South. In 2017, ISOC eventually withdrew the charges and the Pattani Provincial Prosecutor later ended the criminal prosecution of the three prominent human rights defenders. This move came after strong pressure from civil society organisations (CSOs) and also came at a time when Thailand was heading to the UPR process.

In 2020, Danai Usma, a graffiti artist from Phuket, faced a complaint of a CCA violation from the Airports of Thailand (AOT) for posting on Facebook that there were no COVID-19 screening measures at the national Suvarnabhumi Airport. In 2021, the Court acquitted Danai, stating that Danai posted the text on Facebook without intention to cause public panic or disseminate false information.[53] Danai reflected after the verdict that he spent time for two years defending himself: "It is very annoying. We had the right to criticise the government."[54]

53 TLHR, 2022

54 Matichon, 2021

3d. Putting Pressure on ISPs and Tech Companies

The CCA puts a huge burden on internet intermediaries as some of its provisions impose internet liabilities on ISPs and tech companies. Those who fail to comply with these provisions within a specific time will be prosecuted and face punishment.

Orapin Yingyongpathana, a former policy advocate, explained that, prior to 2007, web boards and online forums were the main platforms for people to express their opinions. When the CCA was enforced, the platform owners and ISPs needed to adopt measures to comply with the Act. The increased responsibilities of these internet intermediaries included monitoring comments on their platforms and identifying internet users. These were a huge burden and against the nature of the internet. Moreover, considering big data that flows via the internet, it is impossible to monitor comments and keep surveillance 24 hours a day. As a result, local and small web boards could not bear these burdens and had to end their services. Meanwhile, news online platforms decided to eliminate the comment section under news reports. Only giant web boards and international online platforms survived. The CCA reduced spaces for people to exercise freedom of expression and limited opportunities for local creative ideas or innovation in the online sphere. People moved to express their opinions on international online platforms because it was more difficult to enforce the Act against giant global tech companies.[55]

Further elaborating on this issue, Chiranuch said: "Under the shadow of the restrictive CCA, Prachatai considered that continuing our web board would only increase burdens and [make us] more vulnerable. We decided to close the web board. We felt very terrible because we did not have the potential to protect the rights to privacy of users. If Prachatai had to provide the web board that was restricted based on the CCA, we did not know why we needed to have it. Taken all together, we decided to close our web boards. We notified users one month in advance. It was a loss of space for sharing information and expressing opinion. Calculated in economic values, Prachatai had about hundred of thousands of web board members. We lost high economic values. This hurt. The web board was a virtual community. It was sad. The CCA destroyed the digital creative economy of Thailand and local entrepreneurs."

55 Interview with Asia Centre, 23 March 2022.

However, it was eventually proven that giant international tech companies cannot escape the dark shadow of the CCA amid the pressure of the Thai government. Section 18 of the CCA authorises officials to request user information from service providers. According to updates from the Transparency Centre of Facebook, between January to June 2021 the company received a total 130 requests for data from the Thai government. Of these, 124 of them were legal process requests and 6 were emergency disclosure requests. Throughout 2020, Facebook received a total 267 requests for data from the government. The giant tech company explained that each and every request received from the government is carefully reviewed for legal sufficiency. The company may reject the request or require greater specificity on requests that appear overly broad or vague.[56] In its transparency report, Twitter revealed that from January 2012 to June 2021, it received a total of 103 information requests from the Thai government. The compliance rate of Twitter, however, was at 0%.[57]

Service providers or tech companies delaying or denying compliance with CCA provisions are under pressure. In 2020, Facebook and Twitter faced legal actions under the CCA. The MDES filed legal complaints with the cybercrime police after the giant media companies missed 15-day deadlines to comply fully with court-issued removal orders. It was the first time that the Ministry used the CCA to take action against giant platforms for not complying with court orders. Puttipong Punnakanta, the digital minister, stated that the ministry notified the companies and sent them warnings twice, but they did not comply with any of the requests.[58] The Minister added: "If the companies send their representatives to negotiate, police can bring criminal cases against them. But if they do, and acknowledge the wrongdoing, both parties can reach a settlement by paying a fine."[59]

In response, Facebook threatened to sue the Thai government back for being compelled to block the Royalist Marketplace Facebook group (mentioned earlier), which the government had deemed critical of the country's monarchy. In a statement, the giant tech company said that the blocking requests were serious, broke international human rights law,

56 Facebook, 2021

57 Twitter, 2021

58 BBC, 2020

59 Tanakasempipat and Thepgumpanat, 2020

and caused a chilling effect on people's ability to express opinions.[60] This was a very rare move for Facebook to sue the Thai government as the giant platform had been compliant with Thai laws.

Reacting to Facebook's lawsuit threat, Prime Minister Prayut insisted that Facebook must abide by Thai law, adding that he was not fazed by the social media giant's threat to sue the government for blocking access to accounts deemed insulting to the monarchy.[61]

In 2021, further pressure was placed on Facebook. Nangnoi Assawakittikorn, an ultra royalist, submitted a petition to MDES Minister Chaiwut Thanakamanusornasking for the government to investigate the business operations of Facebook in Thailand. The petition asked the government to investigate issues around Facebook, including paying tax and running business operations that are deemed to affect national security and neutrality. After receiving the petition, the Minister responded that Facebook did not comply with all Thai legislations and that the government was looking into this matter.[62]

Commenting on this issue, a digital expert said: 'Social media platforms have to comply with the Act for their survival. If they do not, they will be punished or their licence may be revoked. They are not happy and hesitate with this law. This Act made them uncomfortable."[63] Thitirat Thipsamritkul, a law professor from Thammasat University, added: "It is widely known in this field that ISPs always hesitate to comply with requests of the authorities under the CCA. They not only have to comply with the Thai legislation, [but also] adhere to international standards. Besides, ISPs need to keep user trustworthiness and prove to their investors that they run business based on ethics. There are many things for ISPs to consider."[64]

60 Iyengar, 2020
61 Bangkok Post, 2020
62 Prachatai, 2021
63 Interview with Asia Centre, 24 March 20220
64 Interview with Asia Centre, 5 April 2022

Pavin, who was prosecuted and whose Facebook group was shut down under the CCA, further shared an interesting point: "Online platforms were requested by the Thai government to take down undesirable content and they had different responses. These different responses by social media platforms could [be attributed to] their selling points and tolerance [of] content that make the government worry. Facebook [was less tolerant] than Twitter. Twitter dared to take risks and was not afraid. I was comfortable posting on Twitter. I was not afraid that my post would be removed or my account would be closed. But, I was concerned when I posted on Facebook."

During an interview with a giant tech platform, Asia Centre noted that tech companies were in a tricky position. These online platforms attempted to balance between complying with provisions of the CCA and following their own internal guidelines. A tech company representative stated: "The CCA is a challenging legislation in large part and [is] unpredictable. Under the CCA, the government forces tech companies to restrict content for them. The companies cannot push [back] so much [against] the government. It could be counterproductive. However, the platform committed itself to freedom of expression and rights of users. Its policy was grounded on international human rights laws including Guiding Principles on Business and Human Rights (UNGPs), the ICCPR, and the International Covenant on Economic, Social and Cultural Rights (ICESCR)."

Aside from these, the CCA also created an economic burden for tech companies, as reflected in the case of a major mobile phone provider. In a 2016 seminar, the DTAC company said that service provider companies needed to introduce measures to prevent punishment under the CCA. They had to establish an investigating team and needed some investment to resolve the issue, resulting in a redirection of investment away from service development and new technologies.[65]

Moreover, Section 26 of the CCA requires service providers to retain log file data of internet users for at least 90 days and up to 2 years if necessary. This requirement increased business operating costs, especially for small and medium-sized enterprises (SMEs),

65 iLaw, 2016b

because organisations had to invest in hardware and software systems to keep computer data. The software alone can cost around THB 100,000 (USD 2,947). The whole system cost between one to ten million baht (USD 29,000 - 290,000).[66] This was a big financial burden on ISPs.

66 Charoen, 2012

IV. RECOMMENDATIONS

This section outlines key recommendations that can be discussed with stakeholders such as the government, parliamentarians, CSOs, tech companies, and the National Human Rights Commission of Thailand to find solutions for upholding and safeguarding digital rights. The recommendations are articulated as calls for action, and can be used as submissions to international human rights mechanisms. In this way, these recommendations can serve to protect and promote digital rights in Thailand.

Government

- Use the CCA only to tackle real cybercrime committed with features of computer systems such as virus, spyware or malware, rather than abuse the Act to manipulate online content or prosecute legitimate expression in the online space.
- Stop using the CCA together with the tough penalties of the Penal Code with intention to compound punishment.
- The Computer Data Screening Committee specified by Section 20 of the CCA should work more effectively, with indicators specified in screening removal requests to avoid arbitrary actions by the authorities.
- Comply with international human rights standards by addressing the recommendations made in the UPR and ICCPR processes.
- Promote digital literacy among all groups of people across the country.

Parliamentarians

- Review and amend Section 14 (2) of the CCA, deleting vague language and providing clear definitions or specifications to avoid arbitrary and overbroad interpretations.
- Lessen the severity of criminal penalties and punish only serious offences that prove to be harmful to public safety.
- Repeal Section 14 (3) of the CCA, which overlaps with provisions in the Penal Code.
- Amend Section 15 from imposing strict liability offence to include the intentionality requirement for committing an offence.
- Amend Section 18 of the CCA to specify that information requests of the authorities must be authorised by the court.
- Section 26 of the CCA should establish a mechanism for protecting privacy and to guarantee that data kept by ISPs or accessed by the authorities are under legal protection.
- Increase transparency and judicial examination in the appointment of the officials who execute the provisions of the CCA.
- Powers for investigation under this Act should be overseen by the court.
- Debate about the CCA prosecutions against political dissidents in the parliament to raise public awareness and criticise the establishment, drawing from their legal protection of parliamentary privilege.

Civil Society Organisations

- Raise public awareness about the CCA and its impact.
- Promote digital literacy among all groups of people across the country.
- Monitor and continue documentation of harassment and prosecutions.
- Provide risk assessment assistance to human rights defenders and activists.
- Engage national and UN human rights mechanisms.

Technology Companies

- Adhere to international human rights standards.
- Honour their mission to protect the exercise of digital rights by users.
- Continue to publicise its transparency reports.
- Work with CSOs in sharing information and advocacy.

National Human Rights Commission of Thailand

- 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.

BIBLIOGRAPHY

'Act on Commission of Offences Relating to Computer' (2007), Krisdika, at: http://web.krisdika.go.th/data/document/ext809/809768_0001.pdf

'Act on Commission of Offences Relating to Computer (Amendment)' (2017), Krisdika, at: http://web.krisdika.go.th/data/document/ext809/809768_0001.pdf

Bangkok Post (2017) 'Online Contact with Regime Critics Banned', at: https://www.bangkokpost.com/thailand/general/1231680/online-contact-with-regime-critics-banned

Bangkok Post (2020) 'PM in War of Words as FB Threatens Lawsuit', at: https://www.bangkokpost.com/thailand/politics/1974467/pm-in-war-of-words-as-fb-threatens-lawsuit

Bangkok Post (2022a) 'Govt Mulls Internet Gateway to Fight Crime', at: https://www.bangkokpost.com/thailand/general/2266939/govt-mulls-internet-gateway-to-fight-crime

Bangkok post (2022b) 'Ex-PM Anand Says Coups Have Retarded Thai Democracy' at: https://www.bangkokpost.com/thailand/politics/2274703/ex-pm-anand-says-coups-have-retarded-thai-democracy

BBC (2020) 'Thailand Prosecutes Facebook, Google and Twitter over Posts', at: https://www.bbc.com/news/technology-54296465

Change.org (2016) 'Stop the Computer Crime Act', at: https://www.change.org/p/7162547/u/18745460

Charoen, Danuvasin (2013) 'Thailand's Computer Crime Act: Security vs. Freedom of Expression', NIDA Case Research Journal, 5(1): 67 - 100

'Convention on Cybercrime' (2001), Council of Europe, at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Facebook (2021) 'Facebook Transparency Centre', at: https://transparency.fb.com/data/content-restrictions/country/TH/

Google (2021) 'Google Transparency Report', at: https://transparencyreport.google.com/youtube-policy/removals?hl=en

iLaw (2014) 'Section 14 of the CCA: Tough Law for Online Defamation' (in Thai), at: https://freedom.ilaw.or.th/blog

iLaw (2016a) 'The Amended Draft of the CCA: Establish the Screening Committee to Close a Website Though It Is Not Illegal' (in Thai), at: https://ilaw.or.th/node/4092

iLaw (2016b) 'DTAC - True Agreed Problem of Defining 'ISPs' and the Single Gateway Will return' (in Thai), at: https://ilaw.or.th/node/4312

iLaw (2018) 'Threaten to Punish against Those who Share: New approach Utilising the CCA to Silence' (in Thai), at: https://ilaw.or.th/node/5044

ITU (2020) 'Individuals Using Internet (% of Population) - Thailand',
ITU, at: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2020&locations=TH&start=1960&view=chart

Iyengar, Rishi (2020) 'Facebook Prepares Legal Action against Thai Government's Order to Block Group', CNN, at: https://edition.cnn.com/2020/08/24/tech/facebook-blocks-thailand-group/index.html

Leesa-Nguansuk, Suchit (2022) 'Thailand 16th Among Google Removal rank', Bangkok Post, at: https://www.bangkokpost.com/business/2249055/thailand-16th-among-google-removal-rank

Matichon (2021) 'The Artist's Case Acquitted for Posting No Screening Measure at Suvarnabhumi Airport, the Court said the Accused Have no Intention' (in Thai), at: https://www.matichon.co.th/local/news_3057547

Nanum, Wassana (2016) 'Activists Protest New Computer Crime Bill', at: https://www.bangkokpost.com/thailand/politics/1162809/activists-protest-new-computer-crime-bill

Paireepairit, Isriya (2012) 'Free Space of Expression: New Media and Thailand's Politics', Germany: Friedrich-Ebert-Stiftung.

PostToday (2020) 'MDES Already Blocked 13,505 URLs for Lèse-Majesté Offences', at: https://www.posttoday.com/economy/news/636943

Prachachat (2019) 'How Coffee Shops Deal with the CCA requiring Log File Retention' at: https://www.prachachat.net/ict/news-379181

Prachatai (2015) 'Supreme Court rules against Prachatai in Internet intermediary liability case', at: https://prachatai.com/english/node/5725

Prachatai (2020a) 'Royalist Marketplace Returns' at: https://prachatai.com/english/node/8748

Prachatai (2020b) 'Court Orders Suspension of Voice TV's online platforms', at: https://prachatai.com/english/node/8859

Prachatai (2021) 'Call for the Government to Investigate Facebook. Its Business Operation Could Affect the National Security' at: https://prachatai.com/journal/2021/09/94941

Reuters (2016) 'Thai PM Defends Cyber Controls as Censorship Concerns Rise', at: https://www.reuters.com/article/us-thailand-cyber-idUSKBN144136

Sabpaitoon, Patpon (2017) 'Prayut Threatens Media Outlets with Strict Cyber Law', at: Bangkok Post, at: https://www.bangkokpost.com/thailand/politics/1364587/prayut-threatens-media-outlets-with-strict-cyber-law

Sawatree, Suksri, Kusonsinwut, Siriphon, and Yingyongpathana, Orapin (2010) 'Situational Report on Control and Censorship of Online Media, through the Use of Laws and the Imposition of Thai State Policies', iLaw, at: https://ilaw.or.th/node/632

Southeast Asian Press Alliance (2009) 'Thai Government Blocks 2,300 Websites; 400 More Face Shutdown', Prachatai, at: https://prachatai.com/english/node/924

Tanakasempipat and Thepgumpanat (2020) 'Thailand Takes First Legal Action Against Facebook, Twitter over Content', Reuters, at: https://www.reuters.com/article/thailand-internet-idUSL3N2GL1HX

Thairath Online (2011) 'A University Student hacked the PM's Twitter', at: https://www.thairath.co.th/content/207112

The Court of Justice (2020) 'Statics of Offences under the 2007 CCA', at: https://oppb.coj.go.th/th/content/category/detail/id/8/cid/2101/iid/166875

The Nation (2018) 'Srivara Makes U-turn On Rap Group', at: https://www.nationthailand.com/in-focus/30357456

TLHR (2017) 'Observations on the MDES Notification Requesting Not To Online Follow Three Persons, at https://tlhr2014.com/archives/4019

TLHR (2022) 'As of April 2022: The Total Number of People Who Are Prosecuted in the Policial Cases Reached 1,808, while the Section 112 Cases Breaks 204 Cases (in Thai), at: https://tlhr2014.com/archives/43253

Tunsarawuth, Sinfah and Mendel, Toby (2010) 'Analysis of Computer Crime Act of Thailand', Thainetizen, at: https://thainetizen.org/wp-content/uploads/2010/07/Analysis-of-Computer-Crime-Act-of-Thailand-By-Sinfah-Tunsarawuth-and-Toby-Mendel.pdf

Twitter (2021) 'Twitter Transparency Report', at: https://transparency.twitter.com/en/reports/countries/th.html

UNHRC (2011a) 'Compilation of UN Information', at: https://www.ohchr.org/EN/HRBodies/UPR/Pages/THindex.aspx

UNHRC (2011b) 'Summary of Stakeholders' Information', at: https://www.ohchr.org/EN/HRBodies/UPR/Pages/THindex.aspx

UNHRC (2015) 'Second Periodic Reports of States Parties Due in 2009: Thailand', at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/224/88/PDF/G1522488.pdf?OpenElement

UNHRC (2017) 'Concluding Observations on the Second Periodic Report of Thailand', at: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsn0o0FGY2xt0pdp5yBVbJo4gsdZhlVrziaLjXLbVlQSTDN0qLBwe559zNYsqKEtBpwSsTUt1UOHhXFewgoB1tdV7tcEMfEDNgEvg9g4RVdd5

UNHRC (2021a) 'Compilation of UN information', at: https://www.ohchr.org/EN/HRBodies/UPR/Pages/THindex.aspx

UNHRC (2021b) 'Summary of Stakeholders' Information', at: https://www.ohchr.org/EN/HRBodies/UPR/Pages/THindex.aspx

World Bank (2020) 'Population, Total - Thailand', World Bank, at: https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TH

We Are Social and KEPIOS (2022) 'Digital 2022: Thailand', DataReportal, at: https://datareportal.com/reports/digital-2022-thailand