Freedom House

FREEDOM ON THE NET 2023

Thailand

NOT FREE

39 /100

A. Obstacles to Access	16 /25
B. Limits on Content	14 /35
C. Violations of User Rights	9 /40

LAST YEAR'S SCORE & STATUS

39 /100 Not Free

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Overview

Internet freedom is severely restricted in Thailand. Ahead of the 2023 general elections, opposition members were discredited through state-sponsored disinformation campaigns, while prodemocracy activists faced arrest, surveillance, and extralegal harassment in retaliation for their online content. Authorities blocked websites and removed content that violated provisions of the restrictive Computer-related Crimes Act (CCA). Internet users continued to be charged with lèse-majesté, with some receiving heavy prison sentences for defaming the monarchy online. Although the repressive emergency decree issued in response to the COVID-19 pandemic lapsed in September 2022, cases continued for individuals previously charged under its provisions.

Following five years of military dictatorship, Thailand transitioned to a military-dominated, semielected government in 2019. The combination of democratic deterioration and frustrations over the role of the monarchy in Thailand's governance triggered massive demonstrations in 2020 and 2021. In response, the regime employed authoritarian tactics, including arbitrary arrests, to squelch the movement. May 2023 polls were the first general elections since the prodemocracy movement started, and voters delivered a clear preference for prodemocracy parties. More than 14 million Thai people voted in favor of the Move Forward Party, which won the election, reflecting strong popular will to embrace its proposal to amend the controversial lèse-majesté law, among other proposals to restore democracy.

Key Developments, June 1, 2022 - May 31, 2023

- A new decree that entered into force in December 2022 imposed stringent requirements on service providers, which are now required to comply with content-takedown requests within 24 hours (see B3).

- State-sponsored disinformation proliferated ahead of the 2023 general elections, with most of this content aimed at discrediting opposition parties and prominent political figures (see B5).
- In January 2023, a prodemocracy activist was sentenced to 42 years in prison, which was later reduced to 28 years, for Facebook posts "defaming" the monarchy (see C3).
- A July 2022 report by Citizen Lab, iLaw, and Digital Reach found that the Thai government has likely deployed Pegasus spyware against prodemocracy advocates, researchers, and politicians (see C5).
- A Vietnamese blogger and YouTuber well known for his online activism was forcibly disappeared in Thailand during the coverage period. Vietnamese state media reported that he had been apprehended while trying to cross the border into Vietnam, from which he had fled years earlier due to political persecution over his antigovernment stances (see C7).

A. Obstacles to Access

A1 0-6 pts	
Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**5**/6

Internet access has improved in recent years, mainly because more people are able to go online using mobile phones. As of January 2023, there were 101.2 million mobile connections, an increase from the previous year. [1] The internet penetration rate stood at 85.3 percent. [2]

Speeds have also been increasing. According to Ookla's Speedtest Global Index, in May 2023 the median mobile and fixed-line broadband download speeds stood at 39.12 megabits per second (Mbps) and 202.88 Mbps, respectively. [3]

In February 2020, three private mobile-service providers and two state-owned telecommunications firms submitted bids totaling 100 billion baht ($3.3 billion) for spectrum required to set up fifth-generation (5G) mobile service infrastructure. [4]

After being the first mobile service provider to launch its 5G network, [5] Advanced Info Service (AIS) had over 6.8 million subscribers at the end of 2022, [6] and is operating about 26,000 5G base stations running across all 77 provinces of Thailand. [7]

A2 0-3 pts	
Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

Disparities in internet access persist, largely based on socioeconomic and geographical factors. However, the cost of access has continued to decrease.

According to the National Statistics Office, about 56 percent of internet users spend 200 to 599 baht ($7 to $20) per month to access the internet as of 2018, the most recent available data, while 21 percent pay under 200 baht per month. [8] The 2021 Affordability Drivers Index estimates that 1 gigabyte (GB) of mobile-broadband service costs 1 percent of Thailand's gross national income (GNI) per capita. [9] As of 2020, roughly 9 million of Thailand's roughly 71 million people accessed the internet through free programs. [10]

Some observers expected the rollout of 5G service to increase internet accessibility, expecting the service to feature lower costs; [11] 5G spectrum licenses, however, are more expensive than anticipated. [12]

Government programs have sought to reduce the persistent digital divide between urban and rural areas. [13] Initiated in early 2017, the Village Broadband Internet Project (Net Pracharat) provided broadband internet via wireless and fixed-line access points to villages in Thailand. [14] In November 2022, the National Digital Economy and Society Commission (NDESC) claimed that the Village Broadband Internet Project had deployed free broadband internet in 74,987 villages. [15] To further improve digital inclusion, the NDESC unveiled measures to reduce broadband fees. [16] In 2021, National Telecom announced plans to provide 300,000 free public Wi-Fi hotspots across the country by 2023. [17]

Three mobile service providers—AIS, TRUE, and DTAC—offer free access to online content through zero-rating services, with the latter two part of the Free Basics by Facebook project in Thailand. The program grants free access to entertainment content and social media platforms, including Facebook, Messenger, and Wikipedia, on mobile phones. [18]

A3 0-6 pts	
Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	**5**/6

There were no reports of the state blocking or throttling fixed-line or mobile connections during the coverage period, though the government does have some capability to do so through technical control over internet infrastructure.

National Telecom was formed in 2021 through a merger of CAT Telecom and TOT, both of which are state-owned. CAT Telecom previously operated international telecommunications infrastructure, including international gateways and connections to submarine cable networks and satellites. [19] Access to the international internet gateway was limited to CAT Telecom until it opened to competitors in 2006. [20] While the merger of CAT Telecom and TOT was intended to help the public firms compete with private telecommunications companies, [21] it was also seen by internet freedom groups as part of the government's plan to consolidate control over the country's telecommunication infrastructure.

Since 2006, the military has repeated plans to establish a "national internet gateway" that would allow Thai authorities to interrupt internet access and the flow of information at any time, but it remains unclear how much work, if any, has been done toward this goal. [22]

The Cybersecurity Act centralizes authority over public and private service providers in the hands of government entities (see C6). Although restricting connectivity is not explicitly mentioned, the law makes it easier for authorities to compel service providers to comply with orders to remove material deemed a threat to national security. [23] The law does not provide transparency concerning government

decisions and lacks an effective system of accountability if connectivity restrictions were to be implemented. [24]

A4 0-6 pts	
Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**4** / 6

Service providers face certain obstacles to market entry, and mergers within the telecommunications sector may reduce market competition.

Although 20 ISPs have licenses to operate in Thailand, the largest three control almost 99 percent of the market. According to a December 2022 NBTC report, National Telecom Public Company Limited (NT) led the sector with 67.4 percent, followed by True Internet Corporation Company Limited (TICC) with 27.4 percent, and AIS subsidiary Advanced Wireless Network Company Limited (AWN) with 2.58 percent. [25]

In the mobile sector, AIS subsidiary AWN held a market share of 44.4 percent in early 2023. [26] TRUE held 32.6 percent, and Norwegian-controlled DTAC followed with almost 20 percent in late 2022. [27] AIS and DTAC operate some spectrum under concessions from state-owned TOT and CAT Telecom—an allocation system that does not entirely enable free-market competition.

In November 2021, TRUE and DTAC announced their plans to merge, prompting concerns about the creation of a mobile-service duopoly: [28] according to a March 2022 NBTC study, the merged company would control 49.4 percent of the market, while AIS subsidiary AWN would hold a market share of 47.72. [29] The merger was successfully completed in March 2023. [30] Afterward, the Foundation for Consumers filed a lawsuit against the NBTC seeking the revocation of the body's endorsement of the merger. [31]

A 2017 report by the nonprofit research group Privacy International found that Thai authorities have long held "close relationships with private telecommunication companies and internet-service providers (ISPs) through appointments which starkly

exemplify the revolving door between the government and the private telecommunications sector." [32]

A5 0-4 pts	
Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Following the 2014 coup, the military junta—known as the National Council for Peace and Order (NCPO)—implemented reforms to the regulatory bodies overseeing service providers and digital technology that reduced their independence, transparency, and accountability, and in 2023 these policies or their successors remained in place.

The NBTC, the former regulator of radio, television, and telecommunications, was stripped of its authority, revenue, and independence when the junta-appointed National Legislative Assembly (NLA) passed the NBTC Act in 2017. [33] It endures as a government agency at half its original size, authorized to implement policy set by a commission led by the prime minister and other new entities with overlapping functions. The government has significant influence over the decisions of the NBTC. [34]

The NBTC commissioners are selected in a process that is highly controlled by the government. The February 2021 NBTC Act further removed requirements that NBTC candidates have experience in relevant spheres. [35] NBTC commissioners receive lucrative salaries and have significant influence over the telecommunications sector. [36]

The MDES was established by the NLA in 2016 to replace the Ministry of Information and Communication Technology and is responsible for implementing policy and enforcing the Computer Crime Act (CCA) (see C2). [37] The Commission for Digital Economy and Society (CDES) provides directives to the MDES and is responsible for formulating policy under the 2017 Digital Development for Economy and Society Act. [38] Chaired by the prime minister, the CDES is composed of government ministers and no more than eight qualified experts. [39] It is not a government body and

therefore not accountable to laws that regulate government agencies, though it has authority over the MDES and NBTC. Other bodies that influence policy include the Digital Economy and Society Development Fund and the Office of Digital Economy Promotion.

The Cybersecurity Act created the National Cybersecurity Committee (NCSC), the Cybersecurity Regulating Committee (CRC), the office of the NCSC, and the Committee Managing the Office of the NCSC (CMO). [40] The NCSC develops policy, guidelines, and a code of practice, while the CRC with the support of the CMO administers these policy products. [41] More than half of the members that make up these committees are government officials, with individuals from the same government bodies or authorities occupying positions in all of them, effectively limiting checks and balances and restricting opportunities to ensure accountability and independence. [42] In January 2022, the Personal Data Protection Committee, the committee tasked with implementing the Personal Data Protection Act (PDPA), was established with mainly government officials as members. [43]

B. Limits on Content

B1 0-6 pts	
Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**3**/6

The blocking of content deemed critical of the monarchy is widespread, but a lack of transparency means that the full extent of this blocking is unclear. Websites have also been blocked on grounds of national security, for gambling content, for alleged violations of intellectual property rights, and for hosting unauthorized virtual private network (VPN) services. [44]

The government has never publicly revealed the number of URLs blocked by court orders. However, the MDES reported that during the first nine months of 2022 it obtained court orders to block roughly 4,735 URLs, including 1,816 URLs containing allegedly offensive content to the monarchy. [45] The number of URLs blocked for

online gambling reached 1,830 in 2022. [46] Additionally, the MDES blocked access to 4,035 URLs for national security reasons and 35 URLs for pornographic content. [47] In January 2023, two online lottery websites and mobile apps were blocked, following a request by the MDES. [48] In February 2022, the MDES blocked no112.org, which hosted an online petition calling for the repeal of the lèse-majesté law, citing alleged violation of the CCA and the Gambling Act. [49] According to OONI Probe's tests, access was restored that month, though people reported that the website remained blocked on some networks as of May 2023." [50]

In October 2020, a secret MDES order was discovered; it directed ISPs and mobile-service providers to block four internet protocol (IP) addresses linked to Telegram, a messaging app used by protesters to communicate and organize. [51] In the same month, the government ordered the blocking of Change.org, after a petition calling for the king to be declared persona non grata in Germany was shared extensively on Twitter. [52] The website was made available again after six months. [53]

Websites offering tools for online anonymity and circumvention of censorship, as well as VPNs such as Ultrasurf and Hotspot Shield, [54] have been blocked by ISPs in the past. [55]

B2 0-4 pts	
Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**1** / 4

Users are often pressured by authorities to remove content, while content providers or intermediaries often comply with removal requests to avoid criminal liability (see B3).

The government pressures and intimidates users, publishers, and content hosts to remove content. In June 2022, YouTube and TikTok complied with 100 percent of the Thai government's content removal orders, although it is unclear what types of content were removed. [56] In May 2022, the MDES sought court orders to remove 42

YouTube, Twitter, and Facebook pages that allegedly defamed the monarchy by sharing an ad from the online shopping platform Lazada. [57]

Between January and June 2022, Facebook restricted access to 711 posts allegedly violating Section 112 of the criminal code on lèse-majesté and 1,530 posts in response to reports submitted by the Thailand Food and Drug Administration. [58] According to Google's transparency report for the same period, the government sent 420 requests to remove 1,097 items across various Google services, 77.5 percent of which were removed. [59] All but one of the requests were related to criticism of the government.

Content targeted for removal or blocking by social media platforms includes speech on political, cultural, historical, and social topics. In January 2021, the government ordered YouTube to restrict access to a music video uploaded by Thai activist rap group Rap against Dictatorship, which called for royal reforms and showcased images of the 2020 antigovernment youth-led protests. [60] In July 2022, the song was banned again on YouTube following an MDES lawsuit requesting the suspension of its dissemination for allegedly violating the CCA and threatening national security. [61] In January 2023, access to Royalist Marketplace, a popular Facebook group that features critical discussions about the king, was blocked for Thai-based users for about one hour, "in response to a legal request," according to Facebook. [62]

In June 2021, courts ordered Facebook and ISPs to block or remove eight Facebook accounts run by activists, journalists, and organizations that have been critical of the Thai monarchy, for allegedly spreading "fake news." The accounts were once again accessible as of May 2023. [63]

Under Section 15 of the CCA, social media companies and other content hosts may be penalized if they fail to comply with a government or court order to take down content that is defamatory, harms national security, causes public panic, or otherwise violates the criminal code. [64] Failing to comply with an order is punishable with a fine of 200,000 baht ($5,900) and an additional daily fine of 5,000 baht ($148) until the order is complied with.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	1 / 4

Restrictions on online content lack transparency and are not proportionate to their stated aims. [65] Attempts to challenge restrictions, which are often applied to antigovernment content or coverage of antigovernment activity, have played out in the courts with mixed results.

In February 2023, human rights lawyer and activist Anon Nampa, a founder of the campaign to repeal Section 112, challenged the court's decision to block no112.org, arguing that making a petition to amend or repeal a law is permissible under the constitution. In March 2023, the court upheld its decision, arguing that the campaign's characterization of the monarchy as a "political institution" was illegitimate and disrupted public order. [66]

In a positive development, in February 2021, the Criminal Court reversed a lower court ruling that a video of Thanathorn Juangroongruangkit, leader of the now-dissolved Thai Future party, criticizing the government's COVID-19 vaccine policy be restricted on three platforms for violating the CCA and threatening national security. [67]

The CCA allows the prosecution of providers or intermediaries for disseminating content deemed harmful national security or public order. Under 2017 amendments, the MDES and other bodies were granted the ability to advance blocking requests. [68] The amendments provided some protection for intermediaries through a notice-and-takedown system, but the law still holds individuals responsible for erasing banned content on personal devices. [69]

Section 14(1) of the CCA bans introducing false or distorted information into a computer system; experts understood this to refer to technical crimes such as hacking. [70] However, the clause has been broadly interpreted and used by the government to intimidate and silence critics (see C2). [71]

Strict language in a December 2022 decree that requires intermediaries to determine legality of content on their own [72] incentivizes service providers and social media

platforms to act on every complaint to avoid liability. [73] For complaints lodged by a member of the public, service providers must remove any content allegedly in violation of Section 14 of the CCA within 24 hours. As of December 2022, users may no longer appeal a removal decision.

The 2022 decree also granted the MDES authority to issue removal orders to service providers, without court authorization or judicial oversight. [74] It further narrowed the window to remove national security–related content to 24 hours, from 11 days previously. [75]

B4 0-4 pts	
Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Thailand's restrictive political environment encourages self-censorship. Legal sanctions for activity such as criticizing the government or businesses online are frequently imposed (see C3). The government has made it known that it monitors social media to control political expression. [76] Users who express dissenting views have faced online harassment and intimidation or had their personal information shared and private lives scrutinized (see C7).

Most Thai internet users and journalists self-censor on public platforms when discussing the monarchy because of the country's severe lèse-majesté laws (see C2). This was particularly true after the Constitutional Court ruled in November 2021 that protesters' calls for reform of the monarchy amounted to an attempt to overthrow it (see C1). In the wake of the said ruling, the NBTC warned the media against covering prodemocracy protests and that noncompliant outlets risk criminal prosecution; [77] this led to increased self-censorship by the media and ordinary users. In November 2022, the court expanded the application of Section 112 of the criminal code on lèse-majesté to prohibit other types of speech (see C2).

However, social media remains a space for relatively critical speech. [78] In early 2023, a number of hashtags about the continuous refusal of bail for prisoners convicted of lèse majesté and other political crimes gained popularity (see B8). [79]

B5 0-4 pts	
Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**1** / 4

Online propaganda, disinformation, and content manipulation are common in Thailand. State entities and some political parties are believed to engage in such practices using a variety of means to target the opposition, human rights defenders, and certain segments of the population. Official efforts to combat disinformation are allegedly selective, allowing progovernment campaigns to proceed with impunity.

Manipulated, false, or misleading online content proliferated during the 2023 election period, with most of this content aimed at discrediting opposition parties and prominent political figures. Certain information operations disseminated false information claiming that the Move Forward Party (MFP) had put forth a proposal to abolish the teacher pension system. [80] After the elections, malicious rumors that MFP planned to allow the United States to establish a military base in Thailand circulated; observers claimed that the rumors were connected to the Internal Security Operations Command (ISOC)—the political arm of the Royal Thai Armed Forces. [81]

Women and members of marginalized groups have also been targeted by information operations for their political activities. In 2022, Paetongtarn Shinawatra from the Pheu Thai party was falsely accused of copying a policy from a previous administration in a campaign aimed at undermining her political abilities and casting doubt on the leadership skills of women. [82] In the predominantly Malay-Muslim southern region, information operations targeted Romadon Panjor, a peace activist who later became an MFP candidate, falsely claiming that he held sympathies towards the ongoing insurgency. [83] Throughout 2023, this misleading content linked to a conservative Buddhist organization circulated on social media accounts. The campaign's purpose appeared to be to protest what organizers perceived as pro-Muslim policies by the junta government. [84]

Revelations by lawmakers and others in recent years have pointed to a well-funded information operations team run by the Thai army; it has spread progovernment sentiment, responded to criticism of the government, and targeted members of the political opposition. [85] In May 2022, the Bangkok Civil Court held initial hearings in a case against the government brought by two rights defenders who alleged that the ISOC violated rules on official conduct by disseminating disinformation to manipulate public opinion about them. [86] The court dismissed the case in February 2023, citing insufficient evidence to demonstrate that the ISOC was responsible for the dissemination of information. [87]

The government has invested in efforts to fight misinformation, but in some cases these tools are employed selectively. In February 2022, the cabinet approved a regulation that would establish centers to combat disinformation on social media at the national, ministerial, and provincial levels. [88] The Anti-Fake News Centre, established by the MDES in November 2019 to combat false and misleading information that violates the CCA, [89] continued to identify news considered false, and release "corrections." [90] Some observers have noted that the government does not work to combat disinformation targeting opposition parties. [91] The Anti-Fake News Center has instead targeted users who post content that is critical of those in power (see C3). [92]

B6 0-3 pts	
Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**2**/3

Many outlets struggle to earn enough in advertising revenue to sustain themselves, limiting their ability to publish diverse content.

Discussions on the draft Media Ethics and Professional Standards Promotion Act, which was approved by the cabinet in January 2022, opened in February 2023. [93] The draft law would require media organizations to register with the new government-appointed Media Council, which would oversee their activities and set ethical standards for reporting. Upon any failure to align their activities with those standards, media outlets risk having their licenses revoked and hefty fines, further

limiting their resources. [94] Thai media organizations are critical of the bill, arguing that the regulation would enable further government control over the media. [95]

New value-added tax (VAT) rules that came into effect in September 2021 require foreign digital service providers to pay a 7 percent VAT on sales if they earn more than 1.8 million baht ($53,300) annually. [96]

B7 0-4 pts	
Does the online information landscape lack diversity and reliability?	**2** / 4

The diversity of viewpoints available online is limited by the enforcement of restrictive laws, policies, and practices—including those specifically aimed at controlling online content—as well as by content removals, economic restrictions, and self-censorship. Nevertheless, social networks and digital media provide opportunities for sharing information that would typically be restricted in traditional media, and Thailand has a relatively vibrant social media environment.

State policies, including the designation of Thai as the country's only official language, limit the availability of news sources in regional and indigenous languages. [97] For example, there is no record of news sites producing content in Lao Isaan, even though the Isaan language is spoken by roughly 22 million people in Thailand. [98]

Ahead of the general elections, the Election Commission (ECT) and TikTok partnered to combat misinformation by removing online content that could misinform the public. [99] The collaboration was strengthened by the involvement of COFACT, Thailand's collaborative fact checking platform, which helped ensure that accurate information was available to the public throughout the election process. [100] Meta also set up safeguards to prevent the spread of misinformation. For example, Facebook required advertisers to go through an authorization process and required ads be labelled with "paid for by." [101]

According to DataReportal's Digital 2023 report, there were 52.25 million social media users in Thailand in January 2023. The most popular platforms were Facebook, LINE, TikTok, and Instagram. [102] Amid increasing state oppression and restrictions on civic

space, activists and politically engaged youths continue to make use of social media, particularly Twitter, to express opinions and garner support for democracy and human rights. [103]

B8 0-6 pts	
Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**3**/6

Most social media, chat applications, and online petition sites are available and serve as essential tools for digital activism, though the risk of criminal charges and targeted harassment or violence has discouraged such activism in practice (see C3 and C7).

Ahead of May 2023 elections, hashtags such as #ThailandElection2023 and #**เลือกตั้ง**66 were used to facilitate discussions. [104] Other hashtags from recent years remain prevalent online. For instance, the hashtag #**ยืนหยุดขัง** (#StandToStopImprisonment) calls for the release of political prisoners held in pretrial detention, and #**หยุดคุกคามประชาชน** (#StopHarassingThePeople) is used to raise awareness of human rights violations by the government. Amid crackdowns on protests against the Asia-Pacific Economic Cooperation (APEC) summit in November 2022, the hashtag #bloodyAPEC2022 gained popularity on Twitter. [105]

At least eight internet users have been charged for posts related to the hashtag #**ตามหาลูกประยุทธ์** (#WhereArePrayutsDaughters) accusing the former prime minister of misusing tax payers' money to pay for his daughters' studies and lifestyles in the UK. [106] In November 2022, an internet user was convicted of defamation and under the CCA for commenting under this hashtag. He was initially sentenced to one year in prison and ordered to pay a 40,000 baht ($1,150) fine. Because he pleaded guilty, his sentence was reduced to six months with a two-year suspended sentence and 20,000 baht ($575) fine. [107]

The online petition platform no112.org was blocked during the previous coverage period (see B1). [108] The government also charged individuals for launching online campaigns against the monarchy. Tiwagorn Withiton was charged with sedition in March 2022 for running a campaign on Change.org that called for a referendum on

abolishing the royal institution. [109] In October 2022, Tiwagorn was given a three-year suspended sentence. [110]

A 2022 draft law on the Operations of Not-for-Profit Organizations defines such groups broadly, and contains language so vague that almost any act may violate the law. [111] The bill is yet to enter into force. [112]

Authorities continue to scrutinize the nongovernmental organization Amnesty International, which in 2020 had launched a campaign to end to criminal charges against monarchy-reform protesters. An investigation into the group, prompted by a petition initiated an official in the office of the prime minister that had gained over a million signatures, [113] was ongoing as of March 2023.

C. Violations of User Rights

C1 0-6 pts	
Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**1** / 6

Score Change: The score improved from 0 to 1 because the state of emergency enacted in September 2020 in response to the COVID-19 pandemic lapsed during the coverage period, precluding future charges under it (though existing cases are ongoing).

The 2017 constitution, drafted by the military government following the 2014 coup, enshrines basic rights, but Section 25 stipulates that all rights and freedoms are guaranteed "insofar as they are not prohibited elsewhere in the constitution or other laws," and that the exercise of those rights must not threaten national security, public order, public morals, or any other person's rights and freedoms.

The 2019 National Cybersecurity Act vaguely defines "critical information infrastructure" as accounting for anything related to national security, economic security, martial security, or public order. The act also provides that any organization

can be identified as critical information infrastructure at the discretion of the NCSC. [114]

A state of emergency whose, launched in response to the COVID-19 pandemic, lapsed in September 2022. The designation placed limits on freedom of expression, including online. Individuals continue to face charges under the law, with at least 507 emergency decree-related cases ongoing as of April 2023. [115]

The amended Communicable Diseases Act (CDA) became the primary legislation governing Thailand's COVID-19 response on the expiration of the state of emergency. [116] Thai civil society groups and UN experts have expressed concern about the law's repressive provisions and the lack of transparency around amendments to the CDA approved by the cabinet in September 2021. [117] These amendments had still not been made public as of March 2023.

Thailand's judiciary is independent under the constitution, but in practice the courts suffer from politicization and corruption [118] and often fail to protect freedom of expression. In November 2021, the Constitutional Court ruled that activists' call for royal reform constituted an attempt to overthrow the monarchy, setting a dangerous legal precedent for freedom of speech. [119] Hundreds of people charged with lèse-majesté are in prolonged pretrial detention (see C3). [120]

The Constitutional Court has summoned users for posting critical content, though the courts have also rejected government requests to block content deemed to be threatening to national security or critical of the monarchy and, at times, ruled in favor of free expression in criminal cases brought against individuals (see B3 and C3). [121]

C2 0-4 pts	
Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**0** / 4

Several laws impose heavy criminal and civil penalties for online activities.

The CCA includes provisions that criminalize online activities (see B3). [122] Section 14(3) criminalizes online content deemed to "affect national security." Observers say the broad language has enabled strategic lawsuits against public participation (SLAPPs), in which government officials and large corporations brought forward cases in order to intimidate and silence their critics. [123]

The criminal code imposes additional penalties for legitimate online activities. People can face up to seven years in prison for acts of sedition under Section 116, and lèse-majesté is covered in Section 112. Those charged with lèse-majesté could face up to 15 years in prison. In 2023, the government expanded the scope of lèse-majesté application to encompass any defamatory statements made about previous kings in addition to the current king, queen, and heir apparent or regent (see C3). [124] Defamation is punishable by up to two years' imprisonment sentence or a fine of up to 20,000 baht ($570). [125] Insulting the courts or judges is punishable by up to seven years' imprisonment and a steep fine. [126]

The 2016 Organic Act on the Referendum for the Draft Constitution criminalizes speech, including via texts and online media, that may "instigate trouble in order to cause disorder in the voting" with up to 10 years' imprisonment and a steep fine. [127]

Users have been arrested and charged under the CCA as well as Sections 112 (which addresses lèse-majesté) and 116 (sedition) of the criminal code for social media activities associated with the prodemocracy movement (see B8).

C3 0-6 pts	
Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**0** / 6

Score Change: The score declined from 1 to 0 because several internet users received long prison sentences for their online content, including a prodemocracy activist who was sentenced to 28 years in prison for Facebook posts "defaming" the monarchy.

Authorities continued to exploit Section 14 of the CCA, the criminal code, and other broadly worded mandates to silence opposition politicians, activists, human rights defenders, and civil society groups. During the coverage period, at least 50 lèse-

majesté cases were recorded, with over half of them in response to online commentary. [128]

In January 2023, after a secret trial, prodemocracy activist Mongkhon "Bas" Thirakot was sentenced to 42 years in prison, which was later reduced to 28 years, for Facebook posts "defaming" the monarchy. [129] Mongkhon's sentence was the longest handed down since January 2021, when Anchan Preelert received a reduced sentence of 43 years after pleading guilty to violating Section 112 of the criminal code and the CCA. [130] Anchan was sentenced after uploading audio clips of "Banpot," a radio host critical of the monarchy, to YouTube. [131]

In May 2023, a security officer was sentenced to 15 years in prison, which was later reduced to 7-and-a-half years, for posting Facebook and TikTok content regarding both the former and current kings of Thailand. [132] In March 2023, a member of the Karen ethnic group was sentenced to 12 years in prison for Facebook posts about the neutrality of the king and which invited people to join a prodemocracy demonstration. [133] In April 2023, the verdict in a Section 112 case was overturned by the Court of Appeal, which held that insulting a deceased king affects the public's emotions and may affect national security. The charges were in relation to Facebook posts about King Rama VIII. The defendant was sentenced to five years in prison, which was later reduced to three years and four months. [134] In November 2022, an online user was found guilty of violating Section 112 of the Criminal Code and the CCA, and sentenced to three years in prison, later reduced to a year and half, for commenting on a picture of King Vajiralongkorn in a Facebook group. [135] In December 2022, former parliamentary candidate Worapon "Oat" Anantasak was charged under Section 112 and the CCA for changing his profile picture on the King's birthday, including captions deemed defamatory and insulting to the monarchy. His house was also raided, and his phones and laptop were confiscated. [136]

Lèse-majesté defendants can face multiple prosecutions, with some facing cumulative prison terms ranging from up to 300 years. Student activist Parit Chiwarak faces numerous charges under the CCA, Section 112, and Section 116 over two Facebook posts dating back to December 2020 about King Maha Vajiralongkorn's divorce and questioning permitted uses of a public park. [137] In May 2023, Chiwarak

was indicted under Section 112 and the CCA for online criticism of courts' treatment of political prisoners. [138]

In May 2022, Sombat Thongyoi, a former protest guard for the United Front for Democracy against Dictatorship, was sentenced to six years' imprisonment for royal defamation and violating the CCA over Facebook comments about the king from 2020. [139] He was released on bail in May 2023, with conditions including wearing a monitoring device and not participating in demonstrations or activities that may damage the reputation of the monarchy. [140]

Despite the end of the emergency decree, 514 cases were still ongoing as of April 2023 (see C1). [141] In January 2023, a social media user charged under Section 14(2) of the CCA, was given a suspended sentence of two years for posting about Thailand's COVID-19 screening measures at the Suvarnabhumi Airport. [142] In January 2023, an appeal court overturned a 2021 criminal court decision [143] and gave a social media user a suspended sentence of two years for posting allegedly false information about his experience with Thailand's COVID-19 airport screening process. [144]

Politician Thanathorn Juangroongruangkit faces several charges for criticizing in an online video Siam Bioscience's exclusive production of a COVID-19 vaccine; the company is effectively owned by the monarchy. [145] The charges against him carry a combined sentence of up to 20 years' imprisonment. He was released on bail and his case remained pending as of May 2023. [146]

In June 2022, an individual was sentenced to 12 years in prison over four messages he posted in the Royalist Marketplace Facebook group that allegedly defamed the king. The sentence was reduced to six years after he pled guilty to violating Section 112 of the criminal code and Section 14(3) of the CCA. [147] He was released on bail. Also in June 2022, three social media influencers were indicted for a video promotion for the Lazada e-commerce network in May 2022 which allegedly insulted the monarchy. [148] The prosecutions against two of them commenced in May 2023. [149] Piyabutr Saengkanokkul, a legal scholar and secretary general of the Progressive Movement, was charged under Section 112 in June 2022 over a Twitter post calling for democracy reforms. [150] In November 2022, a court of appeal sentenced a 19-year-old university

student to three years in prison for criticizing former King's Sufficiency Economy principles on Facebook. The court reduced the sentence to a one year and four months suspended sentence. [151]

A Twitter user known as Niranam was arrested in February 2020 for posts about the king and later charged with additional CCA-related offenses. [152] He was eventually released on bail of 200,000 baht ($6,600). [153] In March 2023, he received an eight-year prison sentence and was fined 160,000 baht ($4,600). The sentence was later reduced to a three-year suspended sentence and the fine was halved. Niranam was also prohibited from socializing with individuals who may influence him to commit a similar offense. [154]

In March 2022, Tiwagorn Withiton was charged with sedition in for his involvement in a Change.org petition on abolishing the monarchy (see B8). [155] In October 2022, Tiwagorn was given a three-year suspended sentence. [156]

Private companies and individuals often file defamation SLAPP cases against human rights defenders, activists, and journalists for denouncing corporate impunity online. In April 2023, electric company Gulf Energy filed a defamation lawsuit against academic Sarinee Achavanuntakul [157] after she wrote a Facebook post about the increased cost of energy and the monopoly of power plants in Thailand. [158] In May, she received a Criminal Court summons and could be forced to pay the company 100 million baht ($2.8 million). [159]

There have been some positive developments in cases regarding online speech in recent years. In January 2023, courts dismissed several royal defamation cases against online users who shared social media posts about the king. [160] In December 2022, a criminal court in Bangkok dismissed a criminal defamation case against LGBT+ rights activist Nada Chaiyajit. The case was filed by a politician and businessman and stemmed from social media posts alleging that he had sexually harassed a transgender woman who was employed at his company. [161] The court held that Chaiyajit was justified in undertaking her human rights work. [162] In November 2022, eight people were acquitted of sedition charges linked to a

Facebook page mocking NCPO leaders. The court held that the defendants were exercising their rights. [163]

C4 0-4 pts	
Does the government place restrictions on anonymous communication or encryption?	**2** / 4

The government has attempted to restrict encryption and has seen some success in limiting online anonymity.

In February 2018, the NBTC ordered all mobile service providers to collect fingerprints or face scans from SIM card holders. [164] In October 2019, facial scans became mandatory for SIM-card registration in three southern provinces. [165] Civil society groups expressed concerns about potential privacy infringements and the potential profiling of the local ethnic Malay Muslim population. [166]

Section 18(7) of the CCA enables officials to order individuals to "decode any person's computer data" without a court order and provides grounds to punish those who fail to decrypt on request. [167]

C5 0-6 pts	
Does state surveillance of internet activities infringe on users' right to privacy?	**1** / 6

The government actively monitors social media and private communications with limited, if any, oversight. A complex set of policies aim to control online communication, but the country lacks a legal framework that establishes accountability and transparency mechanisms for government surveillance.

Sections 18(1) to 18(3) of the CCA allow the government to access user-related or traffic data without court order and compel ISPs to decode programmed data. [168]

Government agencies possess a variety of surveillance technologies. In July 2022, an investigation from Citizen Lab, iLaw, and Digital Reach identified at least 30 Thai

human rights defenders, prodemocracy protestors, and monarchy-reform activists whose devices were infected with Pegasus spyware. [169] The investigation was prompted after Thai politicians, activists, and academics received emails from Apple in November 2021 notifying them that "state-sponsored attackers" may have targeted their iPhones. [170] Following this, the MDES minister admitted that some Thai government departments have been using Pegasus spyware for "national security" and to combat drug trafficking. [171]

In November 2022, eight Thai citizens jointly filed a lawsuit against Israeli company NSO Group for violating their rights after their phones were infected by its Pegasus software. [172] The lawsuit was dismissed by a civil court in Bangkok. [173] One claimant indicated they would refile.

A 2020 report by Citizen Lab identified Thailand as a likely customer of Circles technology. [174] Thailand has also obtained licenses to import telecommunications interception equipment from Switzerland and the United Kingdom. [175] According to Privacy International, the licenses indicate the probable acquisition of IMSI (international mobile subscriber identity) catchers—devices that intercept data from all phones in the immediate area regardless of whether they are the focus of an investigation.

Social media monitoring is also of concern in Thailand. The Anti-Fake News Centres collect information from social media, including through the use of artificial intelligence (AI) that is then reviewed by human content monitors (see B5). [176] There are no clear procedural guidelines or independent oversight mechanisms to ensure that collected data are protected. [177] Activists and online journalists were listed on a police watchlist released in July 2022 along with their social media handles. [178]

The ISOC faced heavy criticism during the 2023 elections after it posted online hourly updates on the MFP's activity in the Prachinburi Province, information that was allegedly gathered through surveillance. [179]

The 2019 National Intelligence Act authorizes the National Intelligence Agency (NIA) to obtain from government agencies or individuals any information that will have an impact on "national security," a term that remains undefined (see C6). If this

information is not provided by a government agency or individual, the NIA may "use any means, including electronic, telecommunication devices or other technologies," to obtain it. [180]

C6 0-6 pts	
Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**1** / 6

The Thai government's centralization of internet infrastructure and close relationship with ISPs facilitates surveillance by the authorities. [181]

Section 15 of the CCA effectively encourages service providers to monitor user information, as they can face penalties under Section 14 if they are found to have "intentionally supported or consented to" a given offense. [182] Failure to monitor what is being shared by a user, take down that information, or share the user's information with the government may be seen as support or consent for the activities in question. In addition, CCA amendments allow officials to instruct service providers to retain computer traffic data for up to two years. Providers must otherwise retain data for at least 90 days under Section 26 of the CCA. Failing to retain this data could lead to a fine of up to 500,000 baht ($14,820). [183]

In October 2019, the MDES directed coffee shops, restaurants, and other venues that offer public Wi-Fi to retain the user data including names and browsing history for at least 90 days. [184] The order was intended to preserve data for the Anti-Fake News Centre and to combat the sharing of purportedly false content that is punishable under Section 14 of the CCA or any other law (see B5 and C2).

The 2019 Personal Data Protection Act (PDPA), which fully entered into force in June 2022, [185] outlines how businesses can collect, use, or disclose personal information. [186] The law can apply to data controllers and data processes outside the country if they process the data of people in Thailand. However, the PDPA provides exemptions for certain activities and authorities. Section 4 exempts any activity of a public authority that has national-security responsibilities. It also allows an exception for the House of Representatives, the Senate, or any committee appointed by them. [187]

Under Section 26, the legal obligation to various public interests is considered a lawful basis to process sensitive personal data, including biometric data, without the data subject's explicit consent. [188] In July 2022, the cabinet approved a draft royal decree proposed by MDES that would carve out exemptions from PDPA for some businesses for activities related to national security, public safety, tax collection, international cooperation, and legal procedures. [189] The decree will come into effect one day after it is published in the Royal Gazette. There was no set date for this in mid-2023.

The PDPA lacks significant safeguards for the automated processing of personal data. [190] Though the National AI Ethics Guidelines, approved by the cabinet in February 2021, require that automated systems processing personal data comply with the PDPA, the limits of the legal regime may be insufficient to protect privacy.

The Personal Data Protection Committee (PDPC), which is responsible for implementing the PDPA, was established in January 2022. [191] The PDPC has 16 members; most are current and former government officials, rather than industry or other experts.

A 2012 cabinet decision allowed investigators to intercept internet communications and collect personal data without a court order in certain cases, including those involving CCA violations. Even where court orders are still required, Thai judges typically approve requests without serious deliberation.

The Cybersecurity Act fails to protect individual privacy and provides broad powers to the government to access personal information without judicial review or other forms of oversight. [192] For issues designated as "critical level threats," officials can access computer systems or data and extract a copy of the information collected. No attempt is required to notify affected persons, and no privacy protections govern the handling of collected information. [193]

The Royal Decree on Measures for Protection and Suppression of Technology Crimes B.E. 2566 took effect in March 2023. [194] The decree allows telecommunication companies to provide user data to the police and other approved agencies.

In recent years, Facebook, [195] Twitter, [196] and Google [197] have reported a handful of government requests to access user data.

C7 0-5 pts	
Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**2** / 5

Prodemocracy activists and individuals who criticize the monarchy have been subjected to doxing, online harassment, extralegal intimidation, and violence in an apparent connection with their online actions. The whereabouts of previously forcibly disappeared activists remain unknown.

Several online journalists were injured while reporting on 2021 prodemocracy protests, which police often repressed with violence. [198] Police also violently repressed journalists covering the dispersal of a protest march that was proceeding towards the site of the APEC meeting in Bangkok in November 2022. Journalist Sutthipath Kanittakul of the online news agency the *Matter* was attacked with a baton and kicked in the head by riot police as he was broadcasting scenes from the crowd. Waranyu Khongsathittum of the *Isaan Record* was likewise punched and kicked before he was arrested. [199] Freelance photojournalist Chalinee Thirasupa received an eye injury from a glass of bottle thrown by the police towards a group of photographers. [200] The *Matter* filed a lawsuit against the national police force over the violence. [201]

Prodemocracy activists who are vocal online, including Sirawit Sertiwat, Ekkachai Hongkangwan, and Pavan Chachavalpongpun, have faced violent attacks inside and outside Thailand during previous coverage periods. [202] The Thai police have not conducted thorough investigations into these incidents and have sometimes halted investigations, [203] blaming the activists for the attacks perpetrated against them. [204]

Individuals who criticized the monarchy receive online and offline threats and intimidation (see B2 and C3). Some participants in the Royalist Marketplace Facebook group have been doxed on social media, threatened by police, or threatened with the loss of their jobs. [205] In 2021, promonarchy users created two Google Maps

documents containing the data of 500 perceived opponents, who they intended to report for engaging in lèse-majesté. [206]

Women in politics receive online abuse, harassment, and gendered defamation, as do women rights activists and gender-nonconforming activists. [207]

In April 2023, Duong Van Thai, a well-known Vietnamese blogger and YouTuber, disappeared in Thailand. Shortly after, Vietnamese state media reported that he had been apprehended while allegedly attempting to cross into Vietnam. [208] Duong Van Thai had left Vietnam in 2018 due to concerns of political persecution resulting from his online activities criticizing the Vietnamese government and the leaders of the Communist Party of Vietnam (CPV). He had previously been granted refugee status by the United Nations. [209]

C8 0-3 pts	
Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**2**/3

While a number of cyberattacks occurred during the coverage period, civil society groups, journalists, and HRDs were not routinely affected by state-sponsored technical attacks in response to their work.

In November 2022, amid the APEC meeting in Bangkok, at least 44 individuals, including activists, civil society members, and Thai refugees, received notifications from Facebook that their accounts may have been targeted by state-sponsored actors. [210]

Major organizations, including high-level government bodies, political parties, and defense and energy institutions, frequently face technical attacks, as do private-sector entities and individuals. [211] According to an August 2022 NCSC report, the number of cyberattacks has increased in recent years. The report indicates that the health care industry, web hosting companies, and data center owners were frequently targeted. [212] In April 2023, the personal information of 55 million Thais, including ID card numbers, dates of birth, addresses, and phone numbers, was stolen from the

Immunization Centre operated by the Public Health Ministry. The suspect, Sgt. Lt. Khemrat Boonchuay, a member of the Royal Thai Army's information operation division, was arrested and charged under the CCA for importing false computer data and additional charges related to national security. [213]

In May 2023, reports surfaced that Dark Pink, a hacking group that frequently targets organizations in the Asia-Pacific region, had targeted a Thai military body with a cyberattack. [214]

The Cybersecurity Act came into force in May 2019. [215] The law aims to protect against, address, and mitigate cybersecurity threats. [216] However, the text fails to protect online freedom and privacy. For example, telecommunications and technology firms designated as operating critical information infrastructure must monitor and report all threats to the government as they develop, which could include sharing confidential information.

In December 2022, Thailand's Personal Data Protection Committee (PDPC) issued the Notification on the Criteria and Procedures for Handling Personal Data Breaches. [217] The notification provides a definition of personal-data breach and outlines a data controller's responsibilities upon receiving notification of an actual or suspected personal-data breach.

• • •

Footnotes

1 Simon Kemp, "Digital 2023: Thailand," Data Reportal, February 14, 2023, https://datareportal.com/reports/digital-2023-thailand

2 Simon Kemp, "Digital 2023: Thailand," Data Reportal, February 14, 2023, https://datareportal.com/reports/digital-2023-thailand

3 "Thailand," Ookla Speedtest Global Index, accessed May 31, 2023, https://www.speedtest.net/global-index/thailand.

4 "5G is about to be real," Bangkok Post, February 24, 2020, https://www.bangkokpost.com/tech/1864284/5g-is-about-to-be-real

5 "AIS the first operator to launch 5G," Bangkok Post, February 22, 2020, https://www.bangkokpost.com/business/1862934/ais-the-first-operator-to-...

More footnotes ⊕

On Thailand

See all data, scores & information on this country or territory.

See More ›

Country Facts

Global Freedom Score

36 /100 **Partly Free**

Internet Freedom Score

39 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

No

Social Media Blocked

No

Websites Blocked

Yes

Pro-government Commentators

Yes

Users Arrested

Yes

In Other Reports

Freedom in the World 2023

Other Years

2022

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES

info@freedomhouse.org

PRESS & MEDIA

press@freedomhouse.org