MANUSHYA Empowering Communities | Advancing Social Justice

accessnow

ARTICLE 19

ASEAN Regional Coalition to #StopDigitalDictatorship

THAILAND UPR III 2021 – UPR FACTSHEET

DIGITAL RIGHTS IN THAILAND
#StopDigitalDictatorship

Brief Assessment of the Implementation of the 2nd Cycle UPR Recommendations

During the 2nd UPR cycle, Thailand received 42 recommendations related to digital rights, including 27 recommendations on freedom of expression, of which 5 recommendations are specific to the Computer Crime Act (CCA) and were made by Canada, Iceland, Norway, Spain and Sweden. Other recommendations which can be applied to Thailand's digital space include 7 recommendations on press freedom and access to information; and 8 recommendations on the protection of human rights defenders. Of these 42 recommendations, 22 were supported and 20 were noted. The government also pledged to "bring national legislation on freedom of expression in compliance with international law" and "ensure that the right to freedom of expression is fully respected and its exercise facilitated, including with respect to the drafting and adopting of the new Constitution." However, our assessment of the situations over the past five year suggests that none of the recommendations have been implemented in reality and the Thai government has not followed through with its pledge. Since the last UPR cycle, netizens are experiencing Thailand's growing digital dictatorship. The government has rolled out a number of repressive laws and policies over the digital space and abused the laws to curtail the fundamental online rights of its citizen. Online users, including pro-democracy activists and dissidents, face charges and criminal penalties under the Criminal Code and laws broadly criminalizing "cybercrimes" and threats to "national security", including the 2017 amended Computer Crimes Act (CCA), the State of Emergency to Combat COVID-19 and the 2005 Emergency Decree on Public Administration in Emergency Situation. Tech companies and service providers have been pressured by the government to enforce censorship on their platforms. The country also lacks an adequate data protection law, further putting the right to privacy of the online citizens at risk of abuses and state surveillance.

National Legal Framework related to Thailand's Digital Space

The 2017 Constitution protects the right to freedom of expression under Sections 34 and 36, with limitations relating to national security, public interest, and public health and order. The Constitution also guarantees media freedom without any censorship under Section 35 and only authorizes restrictions if the country is at war. Further, access to information is recognized as a fundamental right under both Sections 41 and 59 of the Constitution. However, the government continues to impose disproportionate and unnecessary restrictions on these rights in the digital space by using a number of repressive provisions and laws, such as Articles 112, 116, 328 to 333 of the Criminal Code. Article 112 of the Criminal Code (lèse majesté) forbids any criticism of the monarchy and the royal family's members and imposes harsh penalties of imprisonment of up to 15 years for each charge. Article 116 is a sedition-like offense enforcing a penalty of up to 7 years' imprisonment, while Articles 326 to 333 of the Criminal Code area criminal defamation offenses. Article 328, in particular, prohibits defamation by means of a document, video, drawing, or "any other means" with up to two years imprisonment and a fine.

Computer Crimes Act, CCA (2017): Section 14 (1) states that a person is liable for their involvement and storage of any *"false information"* on another person; Section 14 (3) strictly bans sharing of any information that *"could threaten national security"* and Section 14 (5) applies penalties to the *"forwarding and sharing of (prohibited) content."* However, the term 'national security' is left undefined, opening doors to the subjective and blanket application of the law. The CCA also applies to the private sector, which clearly indicates the government's intention to insert an authoritarian control over the digital space. Section 15 sanctions any internet service provider (ISPs) that *"cooperates, consents or acquiesces"* to the perpetration of an offense under Section 14, while Section 26 of the CCA oblige ISPs to retain computer traffic data for at least ninety days from the date on which the data is entered into a computer system. If necessary, a competent official may instruct a service provider to retain such computer traffic data for up to two years.

Cybersecurity Act, CSA (2019): This CSA fortifies the State's online monitoring and mass surveillance powers. Brought into force to combat "cyber threats", the Act provides for overbroad powers to executive authorities to monitor online information and search and seize electronic data and equipment that pose threat to the country's *"national security"*, with the term left undefined. When a threat is deemed a "crisis" level, any search or seizure can be undertaken without a court warrant and without access to appeal before the courts. The Act also imposes reporting obligations on Internet Service Providers and a heavy penalty for non-compliance, encouraging extensive monitoring of users by information technology and telecommunications companies (Sections 73 and 74).

Personal Data Protection Act, PDPA (2019): Drafted with reference to the EU's General Data Protection Regulation (GDPR), the PDPA shall safeguard personal data via restricting the collection, use, disclosure, or tampering of data without the owner's specific prior consent. It also outlines third-party responsibilities in data protection and how businesses shall collect, use or disclose personal data. However, these protections are not definite as Section 4 of the PDPA excludes data collected to protect 'national security' under the 2019 Cybersecurity Act. The PDPA does not specifically address the use of Artificial Intelligence (AI) and automation in legal and institutional frameworks. The PDPA shall enter into force in June 2022.

Emergency Decree on Public Administration in Emergency Situation (2005): On 25 March 2020, a State of Emergency was announced to combat the COVID-19 pandemic. Section 9(3) of the decree prohibits the press release, distribution, or dissemination of letters, publications, or any means of communication containing texts which may *"instigate fear amongst the people"* or is intended to distort information that misleads understanding of the emergency situation to the extent of affecting the security of the state or public order or good moral of the people both in the area or locality where an emergency situation has been declared or the entire Kingdom.

This UPR Factsheet was prepared by Manushya Foundation on the basis of the joint UPR submission with Access Now, Article 19, and the ASEAN Regional Coalition to #StopDigitalDictatorship.
Please access the Joint NGO Submission at the following link: https://www.manushyafoundation.org/digital-rights-joint-upr-submission

REALITIES ON THE GROUND

Challenges	Cases, Facts, Comments

Challenge 1: Crackdown on online freedom of expression under the guise of protecting 'National Security' and combating COVID-19-related 'Fake News'

During the 2nd UPR cycle, Thailand received 27 recommendations on the right to freedom of expression, including 5 recommendations specific to the CCA. Only 11 recommendations were accepted and 16 were noted, including the 5 recommendations to amend the CCA.

So far, the government has failed to implement any of these recommendations as it continues to target and silence dissenting voices online and pressure digital tech companies to facilitate their censorship campaigns through the misuse of laws, such as the CCA, the CSA, and the 2005 Emergency Decree.

For more cases and information, please refer to the UPR Factsheet on Civic Space in Thailand.

A series of laws, such as the CCA and the 2005 Emergency Decree, is used under the guise of *"protecting national security"* to prosecute people allegedly sharing "false information" about the government's actions. However, the lack of clarity as to what constitutes information affecting "national security", provoking "fear" or the so-called "fake news" as laid out in these laws opens the door to subjective interpretation, allowing authorities to arbitrarily enforce the provisions and target free expression online, even information that is factually accurate.

The Weaponization of the Computer Crime Act (CCA) & the Creation of the Anti-Fake News Center

Currently, the CCA is being abused to target dissenting online voices under "national security", a term that is interpreted broadly by the government. For instance, most of the complaints investigated by the Ministry of Digital Economy and Society (MDES) are related to national security and politics, as shared by its former Minister in December 2020 during an interview. Among 16,048 cases received from 31 July to 17 December 2020, 6,855 complaints are related to national security and 4,241 complaints are related to politics. **Among the MDES investigations was the case of the former leader of the dissolved Future Forward Party, Thanathorn Juangroongruangkit.** Following his live Facebook broadcast questioning the government's 'royal COVID-19 vaccine deals' in January 2021, the Ministry filed a complaint against him under Article 112 (lèse majesté) and the CCA, and requested the court to order the recorded broadcast be taken down. The order was later lifted by the court on 8 February 2021, citing that *"although Thanathorn discussed that the Siam Bioscience was owned by the King, there existed no statements that obviously defamed or criticized His Majesty. Therefore, there is no obvious or objective indication that his statements might affect the national security as laid out in Article 112 of the Criminal Code"*. Despite this ruling, he still received a formal police summons on 19 August 2021 on charges of lèse majesté and Section 14(3) of the CCA. In another case, Danai Usama was arrested and charged under the CCA's Section 14 (2) on 24 March 2020 for his online post criticizing the lack of screening measures for COVID-19 symptoms at the Suvarnabhumi Airport. His case is still ongoing, with the first hearing held in May 2021.

Additionally, the government established an "anti-fake news" center in November 2019 under the MDES to strictly implement provisions of the CCA, which include monitoring and issuing corrections for "fake news" that directly affects the general public; creates disharmony in society; creates hoax or false myths; or destroys the country's image. The definition of "fake news" and the scope of the center's mandate is, however, overbroad and appears to target critical dissent.

Censorship of Online Media Freedom

The Thai government also attacks media freedom and the journalists' ability to report without undue interference. For instance, the National Broadcasting and Telecommunications Commission (NBTC), under the Broadcasting and Television Business Act, can suspend or revoke the licenses of radio or television operators broadcasting content deemed false, defamatory to the monarchy, harmful to national security, or critical of the government. Due to this strict control over traditional media, news outlets and journalists are now resorting to online platforms, which has led to an expansion of the government's crackdown on the internet. In October 2020, an order was enacted under the Emergency Decree to silence four independent media agencies (VoiceTV, The Standard, Prachatai, and The Reporters) and the youth-led pro-democracy group Free Youth. Consequently, the online media outlet Voice TV was ordered to close down for violating the CCA and the Emergency Decree for covering the pro-democracy protests. The order was later lifted.

The Misuse of the 2005 Emergency Decree during the COVID-19 Pandemic to stop anyone from telling the truth behind #WhatsHappeningInThailand

On 10 July 2021, the government announced Regulation No. 27, issued under Section 9 of the Royal Decree on Public Administration in Emergency Situations B.E. 2548 (2005), effective 12 July onwards. The regulation prohibits any distorted information or news by books, publications or on any other media that *"incite fear among the public, or intentionally distort information to cause misunderstanding in emergency situations which affects the security of the state or the public's good morals across Thailand"*. Violations of this regulation result in imprisonment not exceeding two years, or a fine of up to 40,000 THB (approx. $1240).

REALITIES ON THE GROUND

Challenges	Cases, Facts, Comments

This regulation was followed by a stricter one on 29 July 2021. The new Regulation No. 29, which came in effect the following day, empowered the NBTC to instruct ISPs to track IP addresses from which prohibited information has been posted. The service providers were then required to report findings to the NBTC and to immediately suspend the internet service of end users. Relevant information would be forwarded by the NBTC to the police for further legal action, and online users violating the regulation could be prosecuted under Section 18 of the Emergency Decree, which provides for imprisonment of up to two years and/or a fine of up to 40,000 baht. This regulation came amid a number of recent government actions to combat COVID-19-related "fake news". On 2 August 2021, representatives from major Thai news agencies filed a civil lawsuit against the Prime Minister over the legality, necessity and proportionality of the new Regulation. On 6 August 2021, the Civil Court ordered the suspension of Regulation No. 29 as it contravenes the rights guaranteed under the Constitution. Consequently, on 9 August 2021, PM Prayut Chan-o-cha revoked Regulation No. 29. However, Regulation No.27 still remains in place.

Challenge 2: The Rise of Digital Dictatorship over Tech Companies

The government's instrumentalization of the laws not only limits online freedom of expression of the netizens, but also pressures tech companies to do the same. Tech companies have been on the receiving end of many problematic censorship and data retention demands under the CCA that are in no way in line with the freedom of expressing, access to information, and rights to privacy under international human rights standards.

Tech companies have been subject to repeated State pressure to limit the freedom of expression on its platforms. Failures to comply could result in severe penalities, such as the suspension of their businesses. For example, under the now-revoked Regulation No.29, ISPs also risked losing their operating licenses and could face legal action if they failed to comply with the NBTC. **In another contentious case, a court ordered Facebook and ISPs to block or remove eight Facebook accounts for allegedly spreading 'fake news' on 2 June 2021.** These include the accounts of political commentator in exile Pavin Chachavalpongpun and journalist Andrew MacGregor, both of which are known for their critical comments on government officials and the Thai monarchy. The access to a Facebook group founded by Pavin - the Royalist Marketplace, where Thai netizens gather to freely discuss Monarchy-related issues - was also restricted earlier last year in August under the Computer Crimes Act. It is now the subject of the landmark non-compliance complaint filed by the Thai government against Facebook. The CCA's Section 15 imposes criminal liability on any ISP for content violating Section 14 of the CCA without requiring the need to establish criminal intent on the part of the ISP, which creates a strong incentive to censor. This is the first time CCA was applied to prosecute an online service provider. Facebook then announced that they would legally challenge the government's requests in court. This case is ongoing.

The recent Ministerial Regulations of the Ministry of Digital Economy and Society regarding criteria for the retention of computer traffic data by service providers, enacted under Section 26 of the CCA, is another clear example of the rising digital dictatorship over tech companies. The order was published on the Royal Gazette on 13 August 2021, replacing the previous one issued in 2007. It requires telecommunication and broadcast carriers - including access service providers, host service providers, internet shops, computer software, AI applications, online application stores, social media service providers, content and application service providers, cloud computing service provider, digital service providers - to preserve internet traffic logs for 90 days in general cases or up to 6 months but not longer than 2 years, if required by relevant law enforcement agencies. Internet shops are also required to install CCTV cameras to keep records of their customers. This means that any exchange or publication of information made on Clubhouse, Telegram, Line, Whatsapp, Facebook, Youtube, Instagram or Google Drive are subject to state surveillance. These are among the main platforms used by pro-democracy activists and protesters to communicate and discuss the issues deemed hostile to the government. The service providers are obliged to keep numerous kinds of computer traffic data, including ID of users, users' activities in the system, log-on and log-off, records of attempts to access the system as well as successful and unsuccessful data records, accessed files, etc.

Challenge 3: Harassment, Intimidation and Attacks against HRDs, Civil Society Activists (CSA) and Journalists for their Online Activities

In the previous UPR cycle, Thailand received 9 recommendations on the protection of HRDs, CSOs and journalists. The government supported 6 recommendations and noted 3. The government has thus far failed to effectively implement any of the recommendations as online and judicial attacks against HRDs and journalists have intensified.

The State-sponsored IOs to Promote Disinformation: The Government is sponsoring disinformation, online harassment and smear campaigns against activists. As part of the so-called Information Operations (IO) of the Internal Security Operations Command (ISOC), a coordinated network of military-linked social media accounts have been registered to post messages that echo the pro-government narratives, and discredit the legitimacy and reputation of the HRDs and civil society organizations.

REALITIES ON THE GROUND

Challenges	Cases, Facts, Comments

Thailand's Growing Cyber Army

On 6 September 2020, the Technology Crime Investigation Police Bureau (TCIPB) or "Cyber Police Bureau" was formed, with responsibilities to enforce the CCA and CSA, and to investigate cybersecurity crime, giving more power to the State to crack down on dissenting voices.

In July 2019, Facebook removed 12 accounts and 10 groups over coordinated inauthentic behavior, and in February 2021, it removed an additional 77 ISOC-related IO accounts: 72 Facebook pages, 18 Facebook groups and 18 Instagram accounts. In October 2020, Twitter banned 926 military-related accounts, most of which were created in January 2020, with a noticeable spike of activities concentrated around the dissolution of the Future Forward Party and the subsequent national pro-democracy movement.

In its February 2021 Coordinated Inauthentic Behavior Report, Facebook said it had detected and removed 185 social media accounts, including: 77 accounts, 72 pages, 18 groups on Facebook and 18 Instagram accounts originating in Thailand, which were found to bear links with the ISOC to target audiences in the country's Deep South. The report identifies Coordinated Inauthentic Behaviour as *"coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation"*. The accounts removed often posted messages in favor of the military and asserted a narrative manipulating the public opinions by discrediting the civil societies and political opponents. One of the examples is a Facebook page named Comprehending the operation (รู้ทันขบวนการ), which published a post criticizing the NGOs, labeling them as uncaring of local people unless they can benefit from them financially.

Such patterns of 'cyber army' instigating online disinformation are constantly growing. During a censure debate on August 31, 2021, Move Forward Party MP Nattacha Boonchaiinsawat confirmed the existence of the Thai army's secret IO network by exposing an authentic footage of an army unit inside an office room dedicated to manipulating pro-government sentiments and targeting political opposition figures online. According to an anonymous officer inside the army who sent the clips, this information unit was under the supervision of the Royal Thai Army's Information Operations Center, where the tasks are divided to support the *"mission of Prime Minister Prayut Chan-o-cha"*.

The Corporate Judicial Harassment against HRDs

Due to the absence of proper protective measures, crime reporting and strategic lawsuits against public participation (SLAPP) are repeatedly used by private companies as a weapon to suppress the online activities of HRDs and journalists, when denouncing corporate abuses. Since 2016, Thammakaset, a Thai poultry company has brought at least 39 complaints against 22 HRDs for sharing allegations of labour rights violations. In 2019, Thammakaset filed a series of criminal defamation lawsuits against HRDs Angkhana Neelapaijit, Puttanee Kangkun, and Thanaporn Saleephol who expressed support for other HRDs targeted by the company in defamation cases on Facebook and Twitter.

Challenge 4: The Lack of Data Protection in Legal and Institutional Framework

During the 2nd UPR cycle, Thailand did not receive specific recommendations on data protection. The government's recent adoption of the Personal Data Protection Act (PDPA) is therefore a promising and commendable step towards the protection of digital rights to privacy in Thailand. However, the legislation still lacks a comprehensive protection framework and policies against the government's potential abuses.

The protections laid out in the PDPA provisions are not definite as Section 4 of the PDPA excludes data collected to protect the undefined "national security" under the 2019 Cyber Security Act, and empowers authorities appointed by the government to collect and use data *"to maintain state security, financial security or public safety"*. However, these provisions remain open to subjective interpretations, without sufficient accountability mechanisms in place to conduct an independent oversight of the authorities' implementation of the law, allowing for a blanket and unfettered application of the law.

The Use of Artificial Intelligence in Thailand's Digital Governance

In recent years, the government has placed AI at the center of their plans to expand digital governance and economy, including through the Thailand 4.0 initiative, and the Thailand Digital Government Development Plan. Yet, these efforts have failed to provide sufficient legal safeguards for personal data protection. The PDPA does not specifically address the use of AI and automation, and neither does it distinguish or identify automated and non-automated means of processing consumer data. It also fails to specify consumers' rights to be informed about the existence of automated decision-making and profiling or to know what and how their personal data is being collected and used, which is in violation of their right to privacy.

REALITIES ON THE GROUND

Challenges	Cases, Facts, Comments

Challenge 5: State Mass Surveillance and Infringement of Online Privacy

During the 2nd UPR cycle, Thailand did not receive specific recommendations concerning online privacy, but noted two recommendations on amending the CCA, which includes provisions that invade user privacy. Despite a new CCA was adopted, the situation remains the same over the past five years, with the new CCA and a series of other new laws that permit surveillance and data collection without court order or independent oversight, coupled with the lack of comprehensive protection framework under the PDPA.

The CCA and CSA invest overboard powers to executive authorities to conduct online monitoring and surveillance, as well as to search and seize personal electronic data that is deemed to be compromising the national security, with its definition left under-defined and no independent accountability mechanisms in place. Sections 18 (1) to 18 (3) of the CCA, for instance, grant vast powers to the monitoring bodies, which include the ability to access user-related or traffic data data without court order as well as compelling ISPs to decode programmed data. Furthermore, the nine-person "Computer Data Screening Committee" – of which six members are government-appointed – can authorize executive authorities, including ministers and "competent officials" to block or delete information deemed "contrary to public order or good morals". The CSA, for its part, fortifies the State's online monitoring and mass surveillance power by providing overbroad powers to executive authorities to monitor online information, and search and seize electronic data and equipment where "national security" and the country's "Critical Information Infrastructure" (CII) are compromised. However, both terms are again left undefined. If a threat is deemed to reach the *"crisis"* level, any search or seizure can be carried out in absence of a court warrant and appeals. The Act also leaves out remedy or accountability provisions for rights violations. With these vaguely-defined provisions, the military and members appointed by the military-led Cabinet can freely interpret "national security" or "threat", allowing for abuses and rights violations to perpetuate without effective oversight and safeguard mechanisms.

The COVID-19 Fake News Center under the Department of Special Investigation

In June 2021, another "Fake News Center" was set up under the Department of Special Investigation (DSI, under the Ministry of Justice) to investigate attempts to spread false news online to mislead the public about the Covid-19 situation, which authorities claims could hamper the government's efforts in containing the coronavirus; and surveil on the citizens by collecting data obtained from the investigation. The new Fake News Center therefore risks not only silencing citizens or journalists who report on the realities of the pandemic, but also compromising their rights to privacy in the digital sphere.

Arbitrary Data Collection during the Coronavirus Pandemic

During the COVID-19 pandemic, unprecedented levels of surveillance and data tracing in Thailand blurred the line between disease surveillance and population surveillance. The two government-approved contact tracing apps Mor Chana and Thai Chana store users' personal data while lacking transparent terms and conditions, and without informing how personal data is being used. There has also been increased online data sharing between government agencies. In June 2020, it was revealed via a leaked document that the COVID-19 response center had shared mobile tracking data of individuals with the Ministry of Defense. Concerns raised over the fact that such personal data shared with government agencies not working in the health sector can lead not only to privacy infringement, but can also be misused for unsubstantiated 'national security'-related investigations.

RECOMMENDATIONS

1. Challenge 1: Crackdown on online freedom of expression under the guise of protecting 'National Security' and combating COVID-19-related 'Fake News'

1.1. In line with the 2017 Human Rights Committee Concluding Observations regarding the protection of freedom of expression in Thailand, **repeal or otherwise amend laws and regulations that restrict freedom of expression, independent media, and access to information,** including but not limited to the Computer Crimes Act, the Computer Cyber Security Act, and the Emergency Decrees, to bring them in line with international human rights law.

2. Challenge 2: The Rise of Digital Dictatorship over Tech Companies

2.1. In line with the UN Guiding Principles on Business and Human Rights (UNGPs) and the Global Network Initiative Principles (GNI), **refrain from pressuring tech companies, internet service providers or other telecommunications companies to moderate and remove content online** in contravention of the rights to free expression and information and ensure their compliance with their responsibilities to respect human rights.

RECOMMENDATIONS

2.2. In line with the 2017 Human Rights Committee Concluding Observations regarding the protection of freedom of expression in Thailand, **repeal or amend ministerial regulations under CCA in accordance with international human rights standards**. Tech companies should not be forced to preserve traffic logs that might be used to restrict freedom of expression.

3. Challenge 3: Harassment, Intimidation and Attacks against HRDs, Civil Society Activists (CSA) and Journalists for their Online Activities

3.1. In line with Thailand's obligations under the ICCPR and with respect to the UN Declaration on Human Rights Defenders, **ensure that HRDs, journalists, civil society members, lawyers and academics are able to carry out their legitimate online activities to shed light on human rights violations without fear or undue hindrance, obstruction and judicial or online harassment.**

4. Challenge 4: The Lack of Data Protection in Legal and Institutional Framework

4.1. **Review and amend the Personal Data Protection Act (PDPA) to bring it in line with Thailand's international human rights obligations**, including to remove the exception clause for data collected under the overbroad justification of "national security" (section 4)

4.2. In accordance with the Human Rights Council Resolution 34/7 on the Rights to Privacy in the Digital Age (2017), **amend the PDPA to address AI and automation by developing legal procedures and evidentiary standards for biometrics with care to protect human rights and due process.**

5. Challenge 5: State Mass Surveillance and Infringement of Online Privacy

5.1. **Repeal or otherwise amend laws which provide for overbroad executive powers to infringe on the right to privacy** – including but not limited to the Computer Crimes Act, the Cybersecurity Act and the National Intelligence Act – to bring them in line with Thailand's international human rights obligations.

5.2. In line with the Human Rights Council Resolution 34/7 on the Rights to Privacy in the Digital Age (2017), **ensure the individual's right to privacy is protected in domestic law in line with international human rights law guaranteed under Article 12 of UDHR and Article 17 of ICCPR,** where any interference with privacy must be strictly necessary and proportionate to accomplish a legitimate objective in accordance with international human rights standards

5.3. In line with the Human Rights Council Resolution 34/7 on the Rights to Privacy in the Digital Age (2017), **develop effective safeguards and independent oversight against State abuses of surveillance technologies, data collection and violation of online privacy**, to limit unfettered executive discretion and establish redress mechanisms consistent with the obligation to provide victims of surveillance-related abuses with adequate and effective remedy.

REFERENCES

Article 19, Thailand: Proposed initiatives to combat 'fake news' undermine freedom of expression, (11 June 2021), available at: https://www.article19.org/resources/thailand-fake-news-undermine-freedom-of-expression/

BBC Thai, วัคซีนโควิด: ศาลเพิกถอนคำสั่งให้ลบโพสต์ธนาธรวิจารณ์เรื่องวัคซีนโควิด, (8 February 2021), available at: https://www.bbc.com/thai/thailand-55975966
Department of Special Investigation, DSI assigned to investigate fake news, (2 May 2021), available at: https://www.dsi.go.th/en/Detail/e4b6841de816696224c7e6cd056f3735

Goldstein, Josh A. et al. "Cheerleading Without Fans: A Low-Impact Domestic Information Operationby the RoyalThai Army," Stanford Internet Observatory Online (Report), (8 October 2020), https://stanford.app.box.com/v/202009-sio-thailand?fbclid=IwAR0jVH2iAL_7e5YAZyhGbPyDJu5dNosQJDoHp1_jfwNDDg2n4HBlHxUzav8

Manushya Foundation, Access Now, Article 19, and the ASEAN Regional Coalition to #StopDigitalDictatorship, Joint UPR Submission: Digital Rights in Thailand, for the UN Universal Periodic Review of Thailand (3rd UPR Cycle), 39th Session of the UPR Working Group, (March 2021), available at https://www.article19.org/wp-content/uploads/2021/04/Joint-UPR-Submission-Digital-Rights-in-Thailand.pdf

Manushya Foundation, Thai Civil Court forced Prayut to Repeal his Regulation No. 29 censoring the Truth online!, (10 August 2021), available at: https://www.manushyafoundation.org/post/thai-civil-court-forced-prayut-to-repeal-his-regulation-no-29-censoring-the-truth-online

Matichon, 'ธนาธร' ได้รับหมายเรียกข้อหา 112 กรณีไลฟ์สดวิจารณ์การจัดหาวัคซีน, (19 August 2021), available at: https://www.matichon.co.th/politics/news_2894166

Prachatai English, 185 accounts related to Thai military information operation removed by Facebook, (5 March 2021), available at: https://prachatai.com/english/node/9101

Thai Enquirer, New hashtag trends on Twitter after more details emerge of government's IO network mission, (1 September 2021), available at: https://www.thaienquirer.com/32101/new-hashtag-trends-on-twitter-after-more-details-emerge-of-governments-io-network-mission/

The Royal Thai Government Gazette, Notification of the Ministry of Digital Economy and Society on Criteria for the Retention of Computer Traffic Data by Service Providers B.E. 2561, (13 August 2021), available at: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/188/T_0009.PDF

The Royal Thai Government Gazette, Regulation No. 27 issued under Section 9 of the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005), (10 July 2021), available at: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/154/T_0001.PDF

The Royal Thai Government Gazette, Regulation No. 29 issued under Section 9 of the Emergency Decree on Public Administration in Emergency Situations B.E. 2548 (2005), (29 July 2021), available at: http://www.ratchakitcha.soc.go.th/DATA/PDF/2564/E/170/T_0001.PDF.

UN Human Rights Committee (HRC), Concluding observations on the second periodic report of Thailand, adopted by the Committee at its 119th session (6-29 March 2017), CCPR/C/THA/CO/2, (April 2017), available at: https://www.refworld.org/docid/591e9d914.html

UN Human Rights Council, Resolution 34/7: The right to privacy in the digital age, adopted by the Council in its Thirty-fourth session (27 February – 24 March 2021), A/HRC/RES/34/7, (7 April 2017), available at: https://digitallibrary.un.org/record/1307661

For more information, evidence and data, please refer to the references and/or contact:
Emilie Pradichit, Founder & Executive Director, Manushya Foundation. Email: emilie@manushyafoundation.org; and
Matthew Bugher, Asia Director, ARTICLE 19. Email: matthew@article19.org