1. Introduction

1.1. In this submission, Manushya Foundation, Access Now, ARTICLE 19 and the ASEAN Regional Coalition to #StopDigitalDictatorship examine the compliance of Thailand with the recommendations it received during its 2nd Universal Periodic Review (UPR) cycle, particularly in relation to digital rights including freedom of expression online, privacy rights and data protection, and the protection of human rights defenders (HRDs) for their online activities.

1.2. During the 2nd UPR cycle, Thailand received 34 recommendations concerning digital rights, of which it supported 19 and noted 15. Our assessment demonstrates that the government has failed to implement these recommendations since its last UPR cycle.

1.3. We are concerned with Thailand's growing digital dictatorship, authoritarian policies and abuse of laws aimed at eliminating citizens' basic human rights, including but not limited to, freedom of expression online. Online users 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.

1.4. We are further alarmed at existing freedom of expression restrictions online that lead to unlawful detentions, judicial harassment as well as alleged disappearances of HRDs and pro-democracy activists. Further, we are deeply concerned that the government pressurizes technology companies to enforce censorship and surveillance measures on their platforms. It is also problematic that the country lacks an adequate data protection law while the authorities carry out online monitoring and surveillance in violation of the right to privacy.

1.5. This submission indicates that the recent political and legal developments violate Thailand's international human rights obligations as follows:

- Section 2 examines the government's implementation of UPR recommendations concerning freedom of expression online, independence of the media, and access to information.
- Section 3 discusses the lack of data protection, with the Personal Data Protection Act (PDPA) not specifically addressing the use of Artificial Intelligence (AI) and automation in legal and institutional frameworks.
- Section 4 discusses state surveillance and infringement of the right to privacy.
- Section 5 discusses challenges faced by technology companies in fulfilling their responsibilities to respect human rights in the digital age.
- Section 6 examines Thailand's implementation of UPR recommendations and its compliance with its international human rights obligations in relation to the protection of HRDs, civil society activists and journalists who exercise their fundamental rights online.
- Section 7 includes a set of recommendations to advance the implementation of UPR recommendations received during the 2nd UPR cycle.

An annex provides an overview of the recommendations examined in this submission.

2. Right to Freedom of Expression Online

2.1. During the 2nd UPR cycle, Thailand received 28 recommendations on the rights to freedom of expression and access to information. The government 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." Of the 28 recommendations received, only 13 were accepted and 15 were noted. So far, the government has failed to implement any of the 28 recommendations on freedom of expression.

2.2. 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.

2.3. ***Articles 112, 116, 328 to 333 of the Criminal Code*** – *Article 112 of the Criminal Code* – or the crime of *lèse majesté* - has been frequently abused to impose illegitimate restrictions on freedom of expression online.[1] Article 112 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. In a recent case, Anchan Preelert was sentenced to a record of 87 years in prison for sharing video clips allegedly criticizing the monarchy back in 2015.[2] Her sentence was halved to 43 and a half years after she pleaded guilty to the charge. As of 22 March 2021, 66 lèse-majesté cases have been filed against 76 pro-democracy activists.[3] *Article 116 of the Criminal Code* – a sedition-like offence enforcing a penalty of up to 7 years' imprisonment – has also been abused to target online expression critical of the authorities or the monarchy. As of November 2020, 46 people have been charged under Article 116. Similarly, criminal defamation charges under *Articles 326 to 333 of the Criminal Code* have also been brought against individuals deemed to express opinions and share information critical of the regime online. Article 328 in particular prohibits defamation by means of a document, video, drawing, or "any other means" with up to two years' imprisonment and hefty fines. On 19 November 2020, The Prime Minister announced that the government would enforce "all laws and all articles", possibly including Article 112, against anti-government protesters expressing their demands of removal and reform of the monarchy.[4] Following the PM's call, royalists started to scour the internet and report on alleged cases of *lèse majesté*, targeting protesters.[5] Pro-democracy movement organizers Chonthicha "Lookkate" Jangrew and Panupong "Mike" Chadnok, who is currently detained on a separate 112 charge, have been charged under Article 112 and the Computer Crimes Act, over Facebook posts promoting monarchy reform,[6] emblematic of how authorities pursue multiple charges to compound punishment.

2.4. ***The Weaponizing of the Computer Crime Act*** – The government also monitors and limits free speech via the Computer Crimes Act (CCA) and a new Cybersecurity Act (2019). The CCA imposes charges on a person who circulates "false information" via online means. 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"[7] and Section 14 (5) applies penalties to the "forwarding and sharing of (prohibited) content."[8] Section 16 further establishes that any electronically edited, altered and added picture, which can hurt a person's image, will be penalized. 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 (11,96 cases in total).[9]

2.5. **The misuse of Emergency Decrees** further worsened restrictions on freedom of expression online. The state of emergency to combat COVID-19 was announced on 24 March 2020[10] and it has since been used to judicially harass individuals criticizing the government's measures to contain the pandemic. For example, Danai Usama was arrested and charged under the CCA's Section 14 (2) for criticizing online the lack of screening measures for COVID-19 symptoms at the Suvarnabhumi Airport. His trial will be in May 2021.[11] A user going by the name of "Niranam" was arrested for posting about the King on Twitter following which he was indicted under CCA's section 14(3) and released on bail. The prosecutor later discontinued his case. However, not long after he was charged on more grounds under the CCA. If found guilty, he faces up to 40 years in jail.[12] Further, following the live Facebook broadcast of popular political opposition leader Thanathorn Juangroongruangkit questioning the government's handling of COVID-19 vaccines in January 2021, MDES filed a complaint against him under Article 112 and the CCA, and requested the court to order the blocking of the online clip. On 8 February 2021, the order was dismissed by the court, which informed MDES that single-party inquiry would no longer be allowed, as the court will have to summon the accused to the inquiry before it decides whether or not to order the blocking or closure of online content.[13]

2.6. The government also restrains press independence through the Broadcasting and Television Business Act, which allows the National Broadcasting and Telecommunications Commission (NBTC) to suspend or revoke licenses of radio or television operators broadcasting content that is deemed false, defamatory to the monarchy, harmful to national security, or critical of the government.[14] Due to strict media controls, Thai people increasingly used the digital space to exercise their right to freedom of expression. This has in turn led to a crackdown on online media, in particular since the Thai military-backed government attempts to impose a digital dictatorship on the rights and freedom of Thai people and free media. Through these efforts, the government has sought to prevent people from sharing with the world the truth about **#WhatsHappeningInThailand**, including police violence at pro-democracy protests. 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.[15] 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, though later the order was lifted.[16]

2.7. The authorities have been extensively restricting access to information online and taking down content from online platforms. The exact number of URLs blocked remains unknown. In November 2020, the Minister of DES issued a warning on his Facebook page about posting inappropriate content on social media and claimed that 1,887 illegal URLs have been found between 1 September and 29 October 2020.[17] Additionally, the international petition website change.org was blocked in October 2020, after a petition critical of the monarchy became popular on the platform. The government also requested internet and mobile services providers to block Telegram, a messaging app highly used by youth protesters.[18] The app remains accessible at the time of writing.

2.8. Additionally, the government established an "anti-fake news" center in November 2019, tasked with monitoring "fake news" that 1) directly affects general public; 2) creates disharmony in society; 3) creates hoax or false myths; or 4) destroys the country's image.[19] The definition of "fake news" and scope of the center's mandate is overbroad and appears to be used to target critical dissent. The

center is responsible for issuing "corrections" to any false assertions through its website, social media accounts and news outlets.[20] Additionally, a new cyber police unit with 1,700 officers was approved in May 2020, to monitor cybercrimes, including those related to "fake news". On 6 September 2020, the Technology Crime Investigation Police Bureau (TCIPB) or "Cyber Police Bureau'' was formed, with responsibilities to enforce the CCA and Cybersecurity Act and to investigate cybersecurity crime, giving more power to the police to crackdown on dissenting voices.[21]

2.9. A new social media app Clubhouse and its Thai users are also under monitoring by MEDS. The former Minister in February 2021 warned Thai users not to "abuse the app and violate the rights of other people and cause damage," otherwise they would be prosecuted under the CCA and other laws. This further shrinks online space for users who would like to freely discuss the country's sensitive issues in online chat rooms.[22]

3. The lack of data protection in legal and institutional framework

3.1. During the 2nd UPR cycle, Thailand did not receive specific recommendations on data protection, although there is no adequate legal and policy framework to protect users' data and right to privacy in Thailand.

3.2. The government's recent adoption of the Personal Data Protection Act (PDPA), which will come into full effect on 1 June 2021, can be perceived as a progressive development. The PDPA was drafted with reference to the EU's General Data Protection Regulation (GDPR) and safeguards personal data via restricting the collection, use, disclosure or tampering of data without the owner's specific prior consent. The PDPA also outlines third-party responsibilities in data protection and how businesses shall collect, use or disclose personal data. Nevertheless, these protections are not definite as Section 4 of the PDPA excludes data collected to protect 'national security' under the 2019 Cybersecurity Act.[23]

3.3. There are further loopholes within the PDPA's provisions. Section 4 of the Act empowers the Parliament as well as the committee and authorities appointed by the government to collect and use data "to maintain state security, financial security or public safety."[24] These provisions remain open to subjective interpretations by the authorities, allowing for overbroad application of the law, without providing for sufficient accountability mechanisms, including independent and impartial oversight of authorities' implementation of the law.[25]

3.4. 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 regulate or provide sufficient safeguards for personal data protection. The PDPA does not specifically address the use of AI and automation and does not distinguish or identify automated and non-automated means of processing consumer data.[26] 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, in violation of their right to privacy. In 2019, the first AI Ethics Guidelines were drafted by the Ministry of Digital Economy and Society (MDES) and are still waiting for approval by the Cabinet.[27] It shed light on ethical principles that are recommended when designing, developing, deploying, implementing or using AI products and services in ways that comply with laws, international standards and respect privacy and human rights.[28] The PDPA critically lacks mandatory obligations towards third parties that would protect personal data and right to privacy.

4. Section 4. State surveillance and infringement of online privacy

4.1. 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.

4.2. In Thailand, a series of laws permit surveillance and arbitrary data search and seizures on the grounds of national security and public order. Sections 18 (1) to 18 (3) of the CCA grant vast powers to the monitoring bodies to access data without court order or other independent oversight. These vast supervisory powers include entering user-related or traffic data as well compelling the Internet Service Providers (ISPs) under section 18 (7) to decode programmed data. Further, under section 20 (3), the "Computer Data Screening Committee" – a nine-person panel of which six are government appointees – is empowered to authorize executive authorities, including ministers and "competent officials" to block or delete information deemed "contrary to public order or good morals". The CCA does not address existing privacy and freedom of expression concerns, but instead, it expands unchecked monitoring of online content by the authorities. The imprecise definition also grants regulatory bodies extensive supervisory powers to eliminate critical dissent or online content that would be regarded lawful under international human rights standards.[29]

4.3. Additionally, the 2019 Cybersecurity Act 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 where "national security" is compromised and to protect the country's "Critical Information Infrastructure" (CII) – where both "national security" and CII are left undefined. The Act establishes insufficient independent monitoring mechanisms - where a threat is deemed "crisis" level, any search or seizure can be undertaken without a court warrant and without access to appeal before the courts. The Act also does not include remedy or accountability provisions for rights violations. Risks for unaccountable violations are imminent as the policy-making bodies determining "national security" or "threat" levels are led by the military and members appointed by the military-led Cabinet.[30]

4.4. The 2019 National Intelligence Act, which came into full effect in April 2019 grants the National Intelligence Agency (NIA) unrestricted powers in compelling ISPs to hand over sensitive personal information whenever the NIA considers the case to be a "national security" threat. The term "national security" still remains undefined and is subjectively interpreted as anything the NIA or government sees fit can fall under this definition, and without adequate, independent or effective oversight mechanisms provided for under the Act. For instance, in situations where the information is not provided by a government agency or individual, the NIA has the authority to "use any means, including electronic telecommunication devices or other technologies" to obtain the particular information.[31]

4.5. Furthermore, problematic national legislation and enforcement mechanisms governing surveillance create the basis for unlawful and excessive surveillance. For example, Malay Muslims living across Thailand have been subjected to discriminatory and disproportionate biometric data collection through facial verification measures and increased CCTV surveillance in the southernmost border provinces of Thailand (or the "Deep South"). The Internal Security Operations Command (ISOC), which is a division within the military, requires Malay Muslims to register their SIM cards via a facial recognition system along with their national identification card details. Individuals who did not comply with these rules by April 2020 experienced targeted mobile network shutdowns in early May

2020.[32] It was also reported that 8,200 CCTVs have been installed within the area under the excuse of "ensuring local population's safety."[33] Currently, the use of the collected personal data remains unknown and there are no legal safeguards in place against potential misuse of the data or violation of the right to privacy. Absence of privacy protections and clear legislation pose a great risk specifically to minority groups and vulnerable individuals. Thus, undue surveillance and the massive collection of data raise serious human rights concerns.

4.6. Equally, the Thai government actively monitors social media and private communications, resulting in illegal intrusion into one's privacy. It was reported that the government possesses various surveillance technologies and licenses to import interception equipment, such as International Mobile Subscriber Identity (IMSI) catchers. These allow authorities to intercept data from all phones in the nearby area unrelated to an operating investigation.[34]

4.7. Lately, the use of hybrid technologies by the Anti-Fake News Center to verify online information and combat allegedly false information have exacerbated privacy and surveillance concerns. Reports indicate that the "Anti-Fake News" center will rely on AI and human monitors to forward the top 10-20 most shared news items or messages on social media including Facebook, Google, Twitter, YouTube to the police for investigation.[35] Meanwhile, 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 contact tracing apps Mor Chana and Thai Chana, approved by the government, store users' personal data while lacking transparent terms and conditions, and without informing how personal data is being used.[36] 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.[37] 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 infringements, but can also abusively be used for unsubstantiated "national security" related investigations or targeting.

5. Rise of Digital Dictatorship over Tech Companies

5.1. During the 2nd UPR cycle, Thailand received and accepted a recommendation to develop and implement a national action plan on business and human rights (NAP-BHR) in line with the UN Guiding Principles on Business and Human Rights (UNGPs). While the government developed a NAP-BHR, the plan does not include any mandatory measures for companies to respect human rights in accordance with the UNGPs Pillar 2. Further, Thailand noted and did not implement two recommendations on amending the CCA, which includes provisions that force ISPs to monitor and take down content deemed "illegal".

5.2. The CCA problematically requires ISPs to retain user data for 90 days and allows for warrantless access to user communication under Section 26.[38] The 2019 National Intelligence Act allows the National Intelligence Agency to compel service providers to hand over information it requests, even if it includes sensitive or personal data.[39] It can result in violation of users' rights, with user data collected without any requirement on authorities to evidence just cause, or to ensure that data requests are made in specific and narrow circumstances in strict compliance with and respect of users' rights. In October 2019, the MDES enforced data retention provisions by ordering coffee shops, restaurants, and other venues that offer public Wi-Fi to retain the data of users, including names, browsing history, and log files, for at least 90 days.[40] Facebook and Google also reported a handful of government requests to access user data.[41]

5.3. The 2019 Cybersecurity Act also imposes reporting obligations on ISPs, encouraging extensive monitoring of users by information technology and telecommunications companies. According to Sections 73 and 74, private enterprises have reporting obligations with respect to cybersecurity incidents and failure to report or submit risk assessment reports could be liable to imprisonment and heavy penalty.[42]

5.4. International tech companies have also been threatened by the government's crackdown on the digital space, being on the receiving end of deeply problematic censorship demands. The government puts illegitimate pressure on ISPs and social media platforms to comply with local laws to take down "illegal" or "fake" content. 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. As a result, intermediaries block or take down material that they fear may be found to be in violation of the law. In August 2020, government pressure caused access to the Royalist Marketplace, a Facebook group openly discussing the Monarchy, to be restricted within Thailand.[43] Facebook and Google were required to comply with the Thai government's orders and remove content relating to the monarchy or authorities that were considered "fake news" and "illegal content." Facebook then announced that they would legally challenge the government's requests in court.[44] This resulted in the government filing a non-compliance complaint against both Twitter and Facebook, which led to a landmark case as for the first time CCA was applied to prosecute an online service provider.[45] This case is ongoing.

6. Harassment, intimidation and attacks against HRDs, Civil Society Activists (CSA) and Journalists for their online activities

6.1. 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 received recommendations.

6.2. Crime reporting and strategic lawsuits against public participation (SLAPP) are repeatedly used as a tool to suppress HRDs and dissidents by authorities and companies. Those who post or comment critical information online face continuous judicial harassment. In 2020, the MDES filed a cybercrime complaint against Pavin Chachavalpongpun, an exiled academic and creator of the Facebook group Royalist Marketplace where a large number of people shared criticisms of the monarchy. This complaint is under investigation. Members of the group have reportedly been targeted with additional CCA complaints as well as intimidation and harassment.[46]

6.3. In absence of anti-SLAPP laws or adequate protective measures, HRDs are vulnerable to lawsuits brought by powerful private actors, 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.[47] 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.[48] Furthermore, in October 2017, the Electricity Generating Authority of Thailand (EGAT), a state enterprise, filed a libel and defamation complaint against environmental activist Prasithchai Noonuan, for criticizing EGAT's plan to build a coal power plant in the Krabi Province on Facebook.[49] The case is still on-going.

6.4. The Government is also sponsoring disinformation, harassment and smear campaigns against activists. ISOC's Information Operations (IO) targeted dissenting voices including activists and academics by establishing military-linked social media accounts, which target posts critical of the

regime with posts, stories and articles aiming to disqualify and discredit the legitimacy and reputation of the HRDs and civil society organizations.[50] In July 2019, Facebook removed 12 accounts and 10 groups over coordinated inauthentic behavior,[51] and in February 2021, it removed an additional 77 ISOC-related IO accounts: 72 Facebook pages, 18 Facebook groups and 18 Instagram accounts.[52] In October 2020, Twitter banned 926 military-related accounts.[53]

6.5. Authorities have also intimidated activists for their online activities. In May 2020, a military officer visited Katima Leeja, a Lisu indigenous rights activist, after she uploaded a video on Facebook criticizing the use of violence by the authorities during a land dispute incident where she demanded an investigation. The police asked about her involvement in land conflict issues and indigenous peoples' rights as well as other personal information.[54] In 2020, 41 similar coercion cases have been recorded by Thai Lawyers for Human Rights, including cases of activists who posted monarchy-related opinions or who just shared monarchy-related news on the internet, and received police visits.[55]

6.6. More tragic, renowned HRDs were reported missing or found dead not long after posting online criticisms of the government or monarchy. Many pro-democracy activists left Thailand as a result of intimidation and stigmatization. Self-exiled activists still face harassment and some have disappeared. In June 2020, Wanchalearm Satsaksit, who faced charges under the CCA, disappeared in Cambodia after posting an online video criticizing the Prime Minister. As of today, no independent, impartial and effective investigation has been conducted into his case, raising suspicions that there may have been State involvement in his disappearance. The aggravations continue to intensify and come in different forms. Individuals have also chosen to self-censor in the face of increased harassment – in the case of student activist Sirin Mungcharoen, she was briefly enforced to withdraw from her social media accounts due to "death threats, sexual harassment as well as online and offline bullying" for a popular video including her protesting.[56]

7. Recommendations to the Thai Government

Manushya Foundation, Access Now, ARTICLE 19 and the ASEAN Regional Coalition to #StopDigitalDictatorship call on the Thai government to respect rights online in law and in practice in accordance with the rights enshrined in the ICCPR, the UN Declaration on Human Rights Defenders and UN Human Rights Council resolutions 22/6, 27/5 and 27/31.

7.1. Regarding freedom of expression online, independence of the media and access to information

a. Decriminalize defamation by repealing sections 326 to 333 of the Criminal Code and enact a stand-alone anti-SLAPP law to ensure legal protections against Strategic Litigation against Public Participation (SLAPP) aiming at silencing dissents, and protect individuals from judicial harassment by the state and corporations. In the meantime, enforce Sections 161/1 and 165/2 of the Criminal Procedure Code and publish statistics on its use to assess its effectiveness in addressing SLAPP cases.

b. Repeal or amend laws and regulations that restrict freedom of expression, independent media, and access to information, including Penal Code Articles 112, 116, the Broadcasting and Television Business Act, the draft Bill on the Promotion of Media Ethics and Professional Standards, the Computer Crimes Act – particularly Articles 14, 15, 16 and 20 –and the Emergency Decrees, to bring them in line with international human rights law. The repeal or amendment process should include effective public consultation.

c. Amend laws addressing hate speech that constitutes incitement to discrimination, hostility, or violence, to bring them in line with international human rights standards and ensure that they are not misused to undermine freedom of expression.

d. When punishing expression as a threat to national security under the CCA, the government must demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence, in line with the Johannesburg principles.[57]

e. End all legal proceedings against, and investigations into, individuals facing harassment, intimidation, or prosecution initiated by state authorities for expression critical of the government and monarchy.

f. Guarantee transparency and access for all persons in Thailand to information, both offline and online, particularly where such information relates to the public interest and impacts upon the individual's right to public participation, including by amending the Official Information Act (1997) or adopting a law to enable the provision of such access.

g. Set up accessible and appropriate mechanisms, judicial and non-judicial; provide among the remedies, fair treatment, impartial compensation or agreement, and the establishment of sufficient grounds to avoid its repetition. Also, implement an evaluation system that regularly screens the existing mechanisms.

7.2. **Regarding the lack of data protection in legal and institutional framework**

a. 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", as presently stated in section 4 of the PDPA.

b. 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; Minimize the amount of and type of data the government and associated service providers collect; Implement measures for accountability and responsibility; Refrain from unlawful interception.

7.3. **Regarding state surveillance and infringement of privacy**

a. 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.

b. Develop effective safeguards against State abuse of surveillance technologies, data collection and violation of online privacy, including by ensuring effective and independent oversight mechanisms are in place 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.

C. 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.

7.4. **Regarding challenges faced by technology companies**

a. 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 in line with the UN Guiding Principles on Business and Human Rights (UNGPs) and the GNI Principles.

b. End all legal proceedings against tech companies facing investigation, charges or prosecution initiated by state authorities for not complying with takedown orders.

c. Provide transparent, detailed and regular updates relating to content moderation requests from government authorities to tech companies and internet providers, including takedown orders, in a public and accessible manner, and information on legal proceedings or action taken against tech companies and internet providers for failure to comply with such requests.

7.5. **Regarding the protection of HRDs**

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

b. Repeal or amend legislation and decrees which unwarrantedly restrict the legitimate work of HRDs in line with the UN Declaration Human Rights Defenders

c. Release unconditionally and immediately HRDs detained for their leadership in the protest movement and end all legal proceedings or investigations against them; Provide effective remedy, including compensation, for unlawful violation of their rights to expression, association, peaceful assembly, liberty and security.

Endnotes

1 See ARTICLE 19 briefing, *Breaking the Silence: Thailand's renewed use of lèse-majeseté charges*, (4 March 2021), available at: https://www.article19.org/resources/thailand-breaking-the-silence/.

2 Manushya Foundation, *87 Years of Jail Time for Violating 112 - It Is Inhuman!,* (20 January 2021), available at: https://www.manushyafoundation.org/post/87-years-of-jail-time-for-violating-112-it-is-inhuman ; Amnesty International, *Thailand: 87-year Prison Sentence Handed in Harshest Lèse-majesté Conviction*, (19 January 2021), available at: https://www.amnesty.org/en/latest/news/2021/01/thailand-87-prison-sentence-lese-majeste/.

3 Among the 76 individuals charged under section 112 in 66 cases: 27 cases were filed by citizens, 5 cases were filed by the Ministry of Digital Economy and Society, 34 cases were filed by the police, with 4 of the accused being under 18-years old. See: Thai Lawyers for Human Rights, **สถิติผู้ถูกดำเนินคดีมาตรา** 112 "**หมิ่นประมาทกษัตริย์**" **ปี** 2563-64, (16 December 2020), available at: https://tlhr2014.com/archives/23983

4 Bangkok Post, *PM: All laws, articles will be used against violent protesters*, (19 November 2020), available at: https://www.bangkokpost.com/thailand/general/2022275/pm-all-laws-articles-will-be-used-against-violent-protesters

5 This Week in Asia, *Thailand protests: royalists scour internet for defamation cases against King Vajiralongkorn*, (29 November 2020), available at: https://www.scmp.com/week-asia/politics/article/3111817/thailand-

protests-royalists-scour-internet-defamation-cases

6 Thai Lawyers for Human Rights, *Lokkate-Mike acknowledge 112 allegations over 'People's Message' post a letter to the King* (25 January 2021) Available at: https://tlhr2014.com/archives/25530#pll_switcher

7 Computer Crime Act B.E. 2560 (2017) (CCA), Section 14(3) available at: http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf

8 Computer Crime Act B.E. 2560 (2017) (CCA), Section 14(5) available at: http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf

9 During his interview, the former Minister for Digital Economy and Society indicated that from 31 July to 17 December 2020, the government online watchdog Facebook page 'Asa jabta' received 39,300 complaints about illegal contents. MDES found evidence for 16,048 cases (41%) while the rest might be deleted before the investigation started. 6,855 complaints are related to national security, 4,241 complaints are related to politics, 2,845 are related to online gambling, 191 complaints about frauds, 101 complaints about fake news, 59 complaints about pornography and 1,765 complaints about other contents.The Bangkok Insight. *Summary of Online Cases in 2020: 7,000 URLs filed for violation of Computer Crime Act, 39 million messages of Fake News found,* (23 December 2020), available at: https://www.thebangkokinsight.com/509993/#:~:text=%E0%B8%AA%E0%B8%B3%E0%B8%AB%E0%B8%A3%E0%B8%B1%E0%B8%9A%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B9%81%E0%B8%88%E0%B9%89%E0%B8%87%E0%B9%80%E0%B8%95%E0%B8%B7%E0%B8%AD%E0%B8%99%E0%B9%81%E0%B8%9E%E0%B8%A5%E0%B8%95%E0%B8%9F%E0%B8%AD%E0%B8%A3%E0%B9%8C%E0%B8%A1,%E0%B8%A2%E0%B8%B9%E0%B8%AD%E0%B8%B2%E0%B8%A3%E0%B9%8C%E0%B9%81%E0%B8%AD%E0%B8%A5

10 Human Rights Watch, *Thailand: State of Emergency Extension Unjustified,* (27 May 2020) available at: https://www.hrw.org/news/2020/05/27/thailand-state-emergency-extension-unjustified#

11 Manushya Foundation, *Internet is Not Free in Thailand - Manushya Report: Freedom on The Net 2020*, (14 October 2020), available at: https://www.manushyafoundation.org/post/internet-is-not-free-in-thailand-manushya-report-freedom-on-the-net-2020 ; Prachatai English, *Artist arrested for posting "Suvarnabhumi Airport has no screening for Covid-19" while in 14-day self-quarantine after his return from Spain*, (27 March 2020), available at: https://prachatai.com/english/node/8432 ; Reuters, *Thai leader to invoke emergency powers as virus infections climb*, (24 March 2020), available at: https://www.reuters.com/article/us-health-coronavirus-thailand-emergency/thai-leader-to-invoke-emergency-powers-as-virus-infections-climb-idUSKBN21B0RV

12 Thai Lawyers for Human Rights, *2020: The Year of Protests, Ceiling Breaking, and Political Lawsuits*, (12 January 2021), available at: https://tlhr2014.com/en/archives/24956 ; Prachatai English, *Netizen faces new charges and up to 40 years in jail over tweets on royalty*, (11 June 2020), available at: https://prachatai.com/english/node/8582

13 Bangkok Post, *Court throws out request to block Thanathorn's clip*, (8 February 2021), available at: https://www.bangkokpost.com/thailand/general/2064655/court-throws-out-request-to-block-thanathorns-clip ; The Reporters, Facebook Video, (19 January 2021), available at: https://www.facebook.com/TheReportersTH/videos/695352251151443/ ; Prachachat, **พุทธิพงษ์ รมว.ดีอีเอส แจ้งความ เอาผิด "ธนาธร" คดี** 112, (20 January 2021), available at: https://www.prachachat.net/politics/news-597843 ; Matichon, **ด่วน! ดีอีเอสแจ้งความเอาผิด 'ธนาธร' ม.112-พ.ร.บ.คอมพ์ ปมไลฟ์เฟซบุ๊กวัคซีนโควิดแล้ว (มีคลิป)**, 20 January 2021, available at: https://www.matichon.co.th/local/crime/news_2538291 ; Thai Post, **'ธนาธร' เฮ! ศาลสั่งเพิกถอนคำร้องดีอีเอส ไม่ระงับคลิปไลฟ์สดวัคซีนโควิด**, (8 February 2021), available at: https://www.thaipost.net/main/detail/92344

14 Broadcasting and Television Business Act B.E.2551 (2008), available at: http://web.krisdika.go.th/data/outsitedata/outsite21/file/Broadcasting_and_Te.levision_Businesses_Act_BE_2551_(2008).pdf

15 Manushya Foundation, *Prayuth's Digital Dictatorship with Online Freedom under Attack,* 19 October 2020, available at: https://www.manushyafoundation.org/post/prayut-s-digital-dictatorship-with-online-freedom-under-attack

16 Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFEnet), *Joint Solidarity Statement- Thailand: Stop Digital Dictatorship Over Online Freedom, #StopDigitalDictatorship, #WhatsHappeningInThailand*, (25 October 2020), available at:

https://www.manushyafoundation.org/statement-th-onlinefreedom-protests

17 Matichon Online, **รมว.ดีอีเอสเผย 1,887 ราย ละเมิดสถาบัน ดำเนินคดี ส่งหลักฐาน ตร.สรุปสำนวนส่งศาล**, (1 November 2020), available at: https://www.matichon.co.th/politics/news_2422367

18 BBC, *Thailand blocks Change.org as petition against king gains traction*, (16 October 2020), available at: https://www.bbc.com/news/world-asia-54566767; Manushya Foundation, *Prayut's Digital Dictatorship With Online Freedom Under Attack*, (19 October 2020), available at: https://www.manushyafoundation.org/post/prayut-s-digital-dictatorship-with-online-freedom-under-attack .

19 From the "Fake News" Center website, https://www.antifakenewscenter.com/%E0%B8%96%E0%B8%B2%E0%B8%A1%E0%B8%95%E0%B8%AD%E0%B8%9A/

20 Manushya Foundation, *Are We Free Online? - Digital Rights in Thailand*, (15 August 2020), available at: https://www.manushyafoundation.org/post/are-we-free-online-digital-rights-in-thailand ; U.S. State Department, *Thailand 2019 Human Rights Report*, 2019, available at: https://www.state.gov/wp-content/uploads/2020/02/THAILAND-2019-HUMAN-RIGHTS-REPORT.pdf ; Reuters, *Thailand unveils 'anti-fake news' center to police the internet*, (1 November 2019), available at: https://www.reuters.com/article/us-thailand-fakenews/thailand-unveils-anti-fake-news-center-to-police-the-internet-idUSKBN1XB48O

21 Bangkok Post, *Cyber cops unit to be set up*, (12 June 2020), available at: https://www.bangkokpost.com/thailand/general/1933404/cyber-cops-unit-to-be-set-up ; Thaiger, *Royal Thai Police form new bureau to investigate cybercrime*, (13 October 2020), available at: https://thethaiger.com/news/national/royal-thai-police-form-new-bureau-to-investigate-cybercrime ; Technology Crime Suppression Division, available at: https://tcsd.go.th/?lang=en ; DES Monitor, Facebook Page, available at: https://www.facebook.com/DESMonitor

22 **กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม**, Facebook post, (16 February 2021), available at: https://www.facebook.com/306279309807142/posts/1138963039872094/ ; Bangkok Post, *Call to be wary of chat rooms*, (18 February 2021), available at: https://www.bangkokpost.com/thailand/general/2069915/call-to-be-wary-of-chat-rooms ; **เจาะลึกทั่วไทย** Inside Thailand, **ขู่** Clubhouse ...**อย่าละเมิด – ความลับไม่มีในโลก | เจาะลึกทั่วไทย** | 18 ก.พ. 64, 18 February 2021, available at: https://www.youtube.com/watch?v=JfBlvRff1gA

23 Human Rights Watch, *Thailand: State of Emergency Extension Unjustified*, (27 May 2020) available at: https://www.hrw.org/news/2020/05/27/thailand-state-emergency-extension-unjustified#; Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, (September 2019), available at: https://www.manushyafoundation.org/study-on-cybersecurity-act

24 Personal Data Protection Act, B.E. 2562 (2019), available at:https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf.

25 Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, (September 2019), available at: https://www.manushyafoundation.org/study-on-cybersecurity-act

26 Fares Alkudmani, *Thailand PDPA v GDPR: The Key Differences,* (11 May 2020), available at: https://secureprivacy.ai/thailand-pdpa-v-gdpr-the-key-differences/

27 OSTDC, *Cabinet takes up artificial intelligence (AI) ethics guidelines*, (25 November 2020), available at: https://ostdc.org/news/5tnnthx9h25pld5iou8m08xhubhxwb ; Bangkok Post, *First draft for AI ethics framed*, (24 October 2019), available at: https://www.bangkokpost.com/tech/1778849/first-draft-for-ai-ethics-framed

28 Ministry of Digital Economy and Society, *AI Ethics Guidelines*, available at: https://www.etda.or.th/getattachment/9d370f25-f37a-4b7c-b661-48d2d730651d/Digital-Thailand-AI-Ethics-Principle-and-Guideline.pdf.aspx?lang=th-TH

29 Computer Crime Act B.E. 2560 (2017), available at: http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf

30 Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, (September 2019), available at: https://www.manushyafoundation.org/study-on-cybersecurity-act

31 Computer Crime Act B.E. 2560 (2017), available at: http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf; Cybersecurity Act, B.E. 2562 (2019), available at:

https://cyrilla.org/en/entity/4nywjpircms?file=1588770279351q8g2xeaybw.pdf&page=1 ; Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, (September 2019), available at:https://www.manushyafoundation.org/study-on-cybersecurity-act.

[32] Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: https://freedomhouse.org/country/thailand/freedom-net/2020 ; Civil Rights Defenders, *Thailand's Facial Recognition policy in the Deep South raises serious human rights concerns,* (18 June 2020),availableat: https://crd.org/2020/06/18/thailands-facial-recognition-policy-in-the-deep-south-raises-serious-human-righ .

[33] Asia Sentinel, *Thai Military Strategy in the Deep South: Surveillance State*, (1 June 2020), available at:https://www.asiasentinel.com/p/thai-military-strategy-in-the-deep; New Mandala, *The Patani Panopticon: biometrics in Thailand's deep south*, (27 May 2020), available at:https://www.newmandala.org/the-patani-panopticon-biometrics-in-thailands-deep-south/.

[34] Privacy International, *Who's That Knocking at My Door? Understanding Surveillance in Thailand*, (January 2017), available at: https://privacyinternational.org/sites/default/files/2017-10/thailand_2017_0.pdf.

[35] Bangkok Post, *Centre goes live to fight fake news*, (12 November 2019), available at: https://www.bangkokpost.com/business/1785199/centre-goes-live-to-fight-fake-news ; Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at:https://freedomhouse.org/country/thailand/freedom-net/2020.

[36] DPEX, *A Comparative Review of Contact Tracing Apps in ASEAN Countries*, (2 June 2020), available at: https://www.dpexnetwork.org/articles/comparative-review-contact-tracing-apps-asean-countries/ ; Bangkok Post, *Thai Covid-19 apps judged invasive*, (20 June 2020), available at:https://www.bangkokpost.com/business/1954287/thai-covid-19-apps-judged-invasive.

[37] Thai Enquirer, *Thai coronavirus response center is sharing mobile tracking data with the Ministry of Defense*, (9 June 2020), available at:https://www.thaienquirer.com/14139/thai-coronavirus-response-center-is-sharing-mobile-tracking-data-with-the-ministry-of-defense/; Bangkok Post, *Govt denies phone tracking*, (9 June 2020), available at:https://www.bangkokpost.com/thailand/general/1931432/govt-denies-phone-tracking.

[38] Section 26 of the CCA stipulates that: "a service provider must retain computer traffic data for a period of not less than ninety days as from the date on which such data enter a computer system, provided that, in the case of necessity, the competent official may order any service provider to retain computer traffic data for a period exceeding ninety days but not exceeding two years as a matter of an individually exceptional case and on an ad hoc basis". See: Computer Crime Act B.E. 2560 (2017), available at: http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf

[39] National Intelligence Act, B.E. 2562, available at: https://www.nia.go.th/FILEROOM/CABFRM01/DRAWER01/GENERAL/DATA0041/00041619.PDF

[40] Freedom House, *Freedom on the Net 2020: Thailand*, 2020, available at: https://freedomhouse.org/country/thailand/freedom-net/2020 ; VOA, *Thailand's Coffee shops told to track, save public Wi-Fi traffic*, (10 October 2019), available at: https://www.voanews.com/east-asia-pacific/thailands-coffee-shops-told-track-save-public-wi-fi-traffic

[41] Google received 2 requests for data regarding 5 users or accounts from January to June 2019, and 1 request for 3 accounts or users between July and December 2019, and 1 request for 2 accounts or users between January and June 2020, while it complied with none. See: Google Transparency Report, *Requests for user information*, 2019, available at: https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:TH;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded
From January to June 2020, Facebook received 164 requests for data regarding 273 users or accounts and provided 74 percent of the data requested. See: Facebook Transparency, *Government Requests for User Data*, 2020, available at: https://transparency.facebook.com/government-data-requests/country/TH

[42] Cybersecurity Act, B.E. 2562 (2019), available at: https://cyrilla.org/en/entity/4nywjpircms?file=1588770279351q8g2xeaybw.pdf&page=1 ; Manushya Foundation, *Thailand's Cybersecurity Act: Towards a human-centred Act protecting online freedom and privacy, while tackling cyber threats*, (September 2019), available at: https://www.manushyafoundation.org/study-on-cybersecurity-act

[43] Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFEnet), *Joint Solidarity Statement- Thailand: Stop Digital Dictatorship Over Online Freedom, #StopDigitalDictatorship, #WhatsHappeningInThailand*, (25 October 2020), available at: https://www.manushyafoundation.org/statement-th-onlinefreedom-protests ; INN News, LIVE!**นายพุทธิพงษ์ ปุณณกันต์ รมว.ดีอีเอส แจ้งความ ปอท**, (23 September 2020), available at: https://www.youtube.com/watch?v=hBN64oSEaZs.

[44] Prachatai, Royalist Marketplace returns, 25 August 2020, available at: https://prachatai.com/english/node/8748 ; The Reuters, Facebook says plans to challenge Thai government demand to block group critical of monarchy, 25 August 2020, available at: https://www.reuters.com/article/us-thailand-facebook-statement-idUSKBN25L0BR.
The former Minister of the Ministry of Digital Economy and Society published 6 posts on Facebook in the same month, publicly threatening Facebook for not complying with government censorship, further exacerbating digital dictatorship. See Bee Punnakanta, Facebook posts, (August 2020), available at: https://www.facebook.com/195119697286323/posts/1923137181151224/; https://www.facebook.com/BeePunnakanta/posts/1923246421140300; https://www.facebook.com/BeePunnakanta/posts/1921569931307949; https://www.facebook.com/195119697286323/posts/1924600384338237/; https://www.facebook.com/BeePunnakanta/posts/1925695094228766?__cft__[0]=AZUr_5mJ2CCz9b-pkNtNFhLp_FGKg73TgRzpwFxJBbH74tu-KgWY_6zo4FyBb_iEl9JH_NsZeGSnr92Tba1l6h5eb60irqubh9Zfo-JGgS4qLkP-eiIZGPthY7BC3y4WG7SofacbwHAyMx6UP6UJBChsvKLbqJgqs1v2DK2EBZDOHA&__tn__=%2CO%2CP-R; https://www.facebook.com/BeePunnakanta/posts/1924542481010694?__cft__[0]=AZW-eLndt0U_Qn4VmMqfsPBGJpuscLbkZarAVkxYVcRktJGsuHWtkGslTZI54GLocIuEQzOv2_uIgbUD0n-83Wuk2IY0CihB_en9YqioaMzI6_VotHPSbkVrMOx0GhPkGgLcKqtqzqQI2hikTvNeB9TxKeYcH5oOecYsdfTue5GpAA&__tn__=%2CO%2CP-R. See also: Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFEnet), *Joint Solidarity Statement- Thailand: Stop Digital Dictatorship Over Online Freedom, #StopDigitalDictatorship, #WhatsHappeningInThailand*, (25 October 2020), available at: https://www.manushyafoundation.org/statement-th-onlinefreedom-protests

[45] Bangkok Post, Govt taking legal action against major social media providers, 24 September 2020, available at: https://www.bangkokpost.com/thailand/politics/1990975/govt-taking-legal-action-against-major-social-media-providers ; The Reuters, Thailand takes first legal action against Facebook, Twitter over content, 23 August 2020, available at: https://www.reuters.com/article/us-thailand-internet-idUKKCN26F0R7. See also: Manushya Foundation, Access Now, ALTSEAN-Burma, Cambodian Center for Human Rights (CCHR), the Institute of Policy Research and Advocacy (ELSAM), PEN Myanmar, and Southeast Asia Freedom of Expression Network (SAFEnet), *Joint Solidarity Statement- Thailand: Stop Digital Dictatorship Over Online Freedom, #StopDigitalDictatorship, #WhatsHappeningInThailand*, (25 October 2020), available at: https://www.manushyafoundation.org/statement-th-onlinefreedom-protests

[46] Thai Lawyers for Human Rights, *2020: The Year of Protests, Ceiling Breaking, and Political Lawsuits*, (12 January 2021), available at: https://tlhr2014.com/en/archives/24956 .

[47] Fortify Rights, *Thailand: Drop Lawsuit by Chicken Company Against Three Women Human Rights Defenders*, (23 November 2020), available at: https://www.fortifyrights.org/tha-inv-2020-11-23/.

[48] Front Line Defenders, *Ongoing judicial harassment of Angkhana Neelapaijit*, available at: https://www.frontlinedefenders.org/en/case/ongoing-judicial-harassment-angkhana-neelapaijit.

[49] Front Line Defenders, *Ongoing judicial harassment of Angkhana Neelapaijit*, available at: https://www.frontlinedefenders.org/en/case/ongoing-judicial-harassment-angkhana-neelapaijit.

[50] Manushya Foundation, *Free Youth & Pro-Democracy Leaders' Twitter Accounts Suspended*, (8 November 2020), available at: https://www.manushyafoundation.org/post/free-youth-pro-democracy-leaders-twitter-accounts-suspended ; Australian Institute of International Affairs, *Are The Thai Army's Information Operations Self-Defeating?*, available at: https://www.internationalaffairs.org.au/australianoutlook/are-the-thai-armys-information-operations-self-defeating/

[51] Facebook, *Removing Coordinated Inauthentic Behavior in Thailand, Russia, Ukraine and Honduras*, (25 July 2019), available at: https://about.fb.com/news/2019/07/removing-cib-thailand-russia-ukraine-honduras/

[52] Facebook, *February 2021 Coordinated Inauthentic Behavior Report*, (3 March 2021), available at: https://about.fb.com/news/2021/03/february-2021-coordinated-inauthentic-behavior-report/

[53] Nikkei, *Twitter bans 926 accounts linked to Thai military manipulation*, (9 October 2020), available at: https://asia.nikkei.com/Politics/Turbulent-Thailand/Twitter-bans-926-accounts-linked-to-Thai-military-manipulation

[54] Thai Lawyers for Human Rights, *TLHR Overall Situation in May 2020*, (18 June 2020), available at: https://tlhr2014.com/en/archives/18582?lang=en ; Prachatai English, *Indigenous woman human rights defender visited by military officer after protest against the alleged violence by forest authorities,* (12 May 2020),
available at: https://prachatai.com/english/node/8510 .

[55] Thai Lawyers for Human Rights, *2020: The Year of Protests, Ceiling Breaking, and Political Lawsuits*, (12 January 2021), available at: https://tlhr2014.com/en/archives/24956

[56] Thai Enquirer, *Sirin 'Fleur' Mungcharoen tells us about the infamous 'black flag' incident in her own words*, (11 March 2020), available at: https://www.thaienquirer.com/9382/sirin-fleur-mungcharoen-tells-us-about-the-infamous-black-flag-incident-in-her-own-words/ ; Twitter post of Fleur dated March 8, 2020, https://twitter.com/fleurs36/status/1236539266479452161

[57] Article 19, *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, 1996, available at: https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf