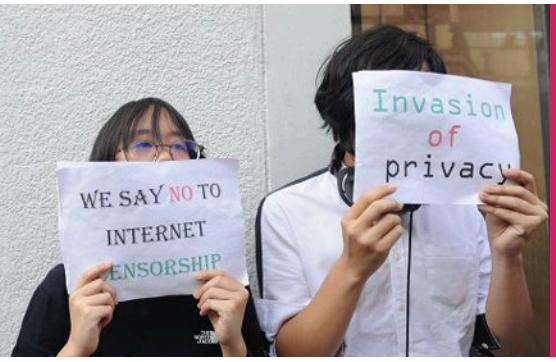
THAILAND UPR IV 2026
UPR FACTSHEET



DIGITAL RIGHTS UNDER ATTACK IN THAILAND

Digital Repression, Online Censorship, State Surveillance, Gendered Violence and Unaccountable AI

Brief Assessment of the Implementation of the 3rd Cycle UPR Recommendations

During the 3rd UPR cycle in November 2021, Thailand received at least 44 recommendations related to freedom of expression, peaceful assembly and association, of which it supported approximately half, including nine specifically addressing digital rights (51.87, 51.88, 51.89, 51.91, 51.93, 51.94, 52.49, 52.54 and 52.55). These included calls to enact a data protection framework consistent with principles of necessity and proportionality, prevent the misuse of cyberspace, and ensure that laws do not unduly restrict freedom of expression and peaceful assembly. Accepted recommendations remained broad in nature; more specific recommendations calling for reform or repeal of the Computer Crimes Act and Section 112 (lèse-majesté) were merely noted.

During the period under review, Thailand has continued to weaponise the Computer Crimes Act, criminal defamation, Section 112, and to a lesser extent Section 116 (sedition) against individuals exercising their right to freedom of expression online. The data protection framework has fallen short of international standards in both scope and enforcement. The ASEAN Regional Coalition to #StopDigitalDictatorship, as well as Freedom House and Manushya Foundation's Freedom on the Net reports have classified Thailand as "Not Free" for five consecutive years. Thailand's 3rd UPR cycle concluded before generative AI tools became widely available in late 2022, and no AI-specific recommendations were made, even though AI is now actively deployed by Thai state authorities in contexts with severe and documented human rights consequences.

This assessment shows that Thailand has failed to implement the accepted 3rd cycle digital rights recommendations. Between 18 July 2020 and 31 August 2026, 2,000 individuals were politically prosecuted across 1,348 cases. Meta restricted over 11,400 items in Thailand across 2025 following government requests, with Section 112 as a central basis; YouTube and TikTok reported near-100 per cent compliance with Thai content removal orders. In August 2025, the National Broadcasting and Telecommunications Commission mandated biometric liveness detection for SIM registration; in January 2026, the Electronic Transactions Committee released a draft notification requiring mandatory identity verification for all social media accounts. A forensic investigation published in July 2022 confirmed Pegasus spyware infections affecting at least 30 activists, human rights defenders and other civil society figures in Thailand between October 2020 and November 2021.

2,000+
people politically prosecuted across 1,348 cases

*between 18 Jul 2020-31 Aug 2026

11,400+
content items restricted by Meta in Thailand, following government requests in 2025

This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

REALITIES ON THE GROUND

Challenges | **Case, Facts, and Comments**

Challenge 1: Weaponisation of Section 112, Section 116, the Computer Crimes Act and criminal defamation against online expression

Thailand's legal cyber arsenal enabling digital dictatorship:
The 2017 Constitution protects freedom of expression under Sections 34 and 36, media freedom under Section 35, and access to information under Sections 41 and 59. These constitutional protections are rendered ineffective in practice by an arsenal of mutually reinforcing criminal laws: Section 112 of the Criminal Code (lèse-majesté), carrying mandatory sentences of three to fifteen years per count; Section 116 (sedition), with a maximum sentence of seven years; criminal defamation provisions (sections 326-333); and the Computer Crimes Act (CCA), which criminalises vaguely defined "false" or security-related online content with up to five years' imprisonment and THB 100,000 fines under Sections 14(1), 14(3), 14(5) and 16; and criminal defamation under Articles 326 to 333 of the Criminal Code, particularly Article 328 covering documents, video, drawings or "any other means" with up to two years' imprisonment.

These provisions are routinely used in combination, multiplying potential sentences for a single act. Section 112 has been identified by successive UPR cycles, UN Special Rapporteurs and UN treaty bodies as incompatible with international standards, but Thailand has failed to reform it. On 7 August 2024, the Constitutional Court dissolved the Move Forward Party (winner of the 2023 general elections with over 14 million votes) on the grounds that its advocacy for Section 112 reform constituted high treason, imposing 10-year political bans on its executive members.



Pro-democracy student activist Tantawan "Tawan" Tuatulanon.
She was sentenced two years in prison under both lèse-majesté and computer crime charges for hosting a Facebook livestream where she critiqued the clearing of a farmers' protest ahead of a royal motorcade.

SOURCE: Thai Lawyers for Human Rights (TLHR) (2022, March)

2,000 individuals politically prosecuted between 18 July 2020 and 31 August 2026.
Of these, TLHR confirmed 293 individuals were charged under Section 112 across 322 cases; 158 individuals under Section 116 across 58 cases; and 224 under the CCA across 244 cases.

Mongkhon "Bas" Thirakhot: 46 years for 27 Facebook posts.
The pro-democracy activist prosecuted for 27 Facebook posts was sentenced to 28 years in January 2023, increased to 50 years by the Court of Appeals in 2024, and reduced by the Supreme Court to 46 years, exceeding the previous record 43.6-year sentence imposed on Anchan Preelert in 2021. He's been held without bail since January 2024.

Arnon Nampa: Potential cumulative sentence of up to 210 years.
Human rights lawyer and pro-democracy activist has remained detained since his first Section 112 conviction on 26 September 2023 and has repeatedly been denied bail. He has faced 14 cases under Section 112, which carries 3 to 15 years in prison per offence. Fourteen convictions at that statutory range could amount to 42 to 210 years before any sentence reductions. His prosecution shows how online criticism can lead to prison: in 2024, he received two separate four-year sentences for Facebook posts under Section 112 and the Computer Crime Act (CCA). By August 2026, his convictions for online posts and public speeches had produced a cumulative sentence of **31 years, 9 months and 20 days.** In 2024, the UN Working Group on Arbitrary Detention found his detention arbitrary and called for his immediate release and reparations.

Tawan: Two-year prison sentence for a Facebook livestream.
Tantawan "Tawan" Tuatulanon, a 25-year-old student activist, livestreamed on Facebook in March 2022 as police cleared a farmers' protest ahead of a royal motorcade. She questioned why the farmers were being moved instead of having their concerns heard. On 31 August 2026, a court convicted her under Section 112 and the Computer Crime Act, treating her livestream as false data affecting national security. She received a two-year prison sentence without suspension and was granted bail pending appeal. Her case shows how online criticism of state action can be prosecuted as both lèse-majesté and a computer crime.

Paul Chambers: Cross-border prosecution of online academic expression.
In April 2025, Thai authorities arrested American academic Dr. Paul Chambers under Section 112 and the Computer Crime Act over an online description of a webinar titled "Thailand's 2024 Military and Police Reshuffles: What Do They Mean?" The description was published by a Singapore-based institute that had invited him to speak. Chambers maintained that he had neither written nor posted it. Although prosecutors dropped the case in May 2025, his visa was revoked, he lost his university job, and he left Thailand after living there for more than 30 years. His case shows how academic material published abroad can trigger prosecution and lasting harm.

This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

REALITIES ON THE GROUND

Challenges | **Case, Facts, and Comments**



Deep South woman human rights defender Anchana Heemmina.
She faced criminal defamation and Computer Crime Act charges for exposing on Facebook about a military camp's unpaid water bill to a mosque. She was later acquitted for the computer crime charge, with the court finding no intent to deceive.

SOURCE: Luke Duggleby / Protection International (2022)

Judicial harassment: SLAPPs against journalists and human rights defenders.
On 27 February 2026, the Minister of Natural Resources and Environment sued The Isaan Record editor **Hathairat Phaholtap** for criminal defamation over Facebook posts about reporting on alleged bribery linked to Thai berry pickers in Finland. He later brought a separate case against editor **Kowit Phothisan** for sharing her post. The minister requested withdrawal of Hathairat's case on 23 March; on 8 June, the Chonburi Provincial Court dismissed Kowit's case, finding that his post was fair criticism on a matter of public interest.

On 8 May 2024, Deep South human rights defender **Anchana Heemmina** posted on Facebook about a military camp's unpaid water bill to a mosque. She promptly corrected an error about the location, yet faced criminal defamation and Computer Crime Act proceedings in 2025. On 6 November 2025, the Narathiwat Provincial Court acquitted her of the computer crime charge, finding no intent to deceive. These cases show how public-interest reporting and online advocacy can carry a legal burden even when the claims fail.

Challenge 2: State surveillance and digital control through platform data access, spyware, information operations and AI-enabled monitoring

Government access to platform user data
Thai authorities can seek information about users and accounts from digital platforms through legal process and emergency requests. When platforms disclose that information, authorities may be able to identify people behind online expression. The volume of requests raises concerns about privacy, especially where there is little public information about who is targeted, why their data is sought, or what safeguards protect political expression. Meta's 2025 figures in the cases column show the scale of this access

Spyware and intrusive state surveillance: Use of Pegasus and commercial spyware against HRDs
The period under review produced the first forensically confirmed evidence of the use of military-grade commercial spyware against Thai activists. A joint civil society investigation identified at least 30 individuals targeted or infected with NSO Group's Pegasus spyware, including at least twelve women. Observed infections took place between October 2020 and November 2021, coinciding with the pro-democracy protests, and the investigation was triggered by Apple notifications sent to Thai civil society in November 2021.



Meta compliance with Thai state data requests: 84.47% from January to June 2025.
Thai authorities submitted 3,452 total requests to Meta in the first half of 2025, comprising 3,403 legal process requests and 49 emergency disclosure requests, covering 6,045 users and accounts. Meta produced data in response to 2,916 requests (84.47% of the requests), functioning as an infrastructure of surveillance that enables the identification, monitoring and prosecution of individuals exercising their right to freedom of expression online.

Jatupat "Pai" Boonpattararaksa's civil claim against NSO Group was dismissed.
Pai brought a civil claim against NSO Group, the developer of Pegasus, seeking to hold the company liable after forensic researchers identified infections on his phone. On 21 November 2024, the Bangkok Civil Court dismissed the claim, finding that the evidence submitted did not sufficiently prove the infection for the purposes of the case. The judgment did not determine which actor operated Pegasus against activists in Thailand.

Arnon Nampa and Yingcheep Atchanont's administrative claim against nine Thai government agencies was admitted for hearing.
Arnon and Yingcheep sued nine State agencies, alleging that officials had unlawfully used Pegasus to access their phones and seeking State accountability. The Central Administrative Court initially declined to hear the claim, but on 27 February 2025 the Supreme Administrative Court ordered that it be accepted. In pleadings reported by iLaw in November 2025, the agencies denied using Pegasus to surveil the two claimants. The Royal Thai Police acknowledged acquiring Pegasus in 2014 but denied using it against them. The case remains unresolved.

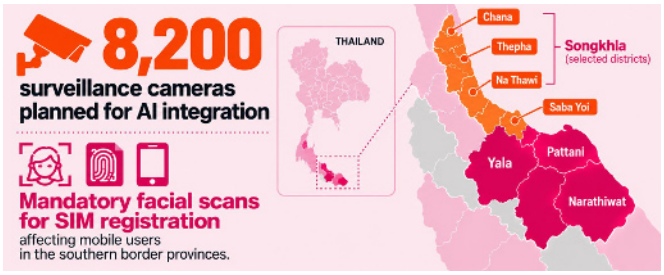
This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

REALITIES ON THE GROUND

Challenges | **Case, Facts, and Comments**

State-led and coordinated information operations

Digital targeting extends beyond commercially procured spyware to include coordinated information operations launching disinformation campaigns to discredit the work of human rights organisations and defenders. Amnesty International reported that during a parliamentary no-confidence debate on 25 March 2025, an opposition parliamentarian disclosed leaked internal documents of a Cyber Team operating under a Joint Command Center run by police and military units including the Internal Security Operations Command (ISOC).



Biometric and AI-enabled surveillance in the Deep South

In the Southern Border Provinces of Yala, Pattani and Narathiwat and the districts of Na Thawee, Jana, Tepa and Sabayoi of Songkla, advanced technologies such as facial recognition systems and predictive policing tools were deployed to monitor and scrutinize the activities of the local Malay Muslim populations. A significant expansion of these surveillance efforts was marked by requiring individuals to provide facial scans to different mobile service providers such as AIS, TrueMove H, and DTAC.

Disinformation campaign against women human rights defenders.

On 11 June 2026, Thailand's Court of Appeal found the state responsible for online smear attacks against women human rights defenders **Angkhana Neelapaijit** and **Anchana Heemmina** on a website controlled by an ISOC unit. It ordered compensation of THB 120,000 and THB 90,000, respectively, and removal of the offending content once the judgment becomes final. The landmark ruling recognised the harm caused by disinformation targeting their human rights work.

In July 2026, Angkhana and Anchana faced renewed online attacks and death threats. Angkhana filed a police complaint on 31 July after false claims about her circulated following the deadly attack in Narathiwat. False allegations and death threats led Angkhana to file a police complaint on 31 July. Their cases show both the possibility of holding state agencies accountable for digital attacks and the urgent need to protect defenders when new threats emerge. The perpetrators of the July attacks have not been established.

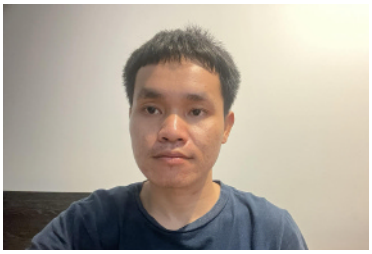
Mandatory biometric SIM verification and identity verification.

Authorities required mobile users in the southern border provinces to register their SIM cards using facial scans, collecting biometric data in a region with a predominantly Malay Muslim population. In January 2020, the government announced plans to add AI to at least 8,200 existing surveillance cameras. The available reporting does not establish that all 8,200 cameras received AI capabilities or that they were linked to the facial-scan database.

Challenge 3: Digital transnational repression and technology-facilitated gender-based violence (TFGBV) against women and LGBTIQ+ defenders

Digital Transnational Repression

Thailand is a regional hub for people fleeing persecution, yet defenders living there remain exposed to digital threats that can cross borders, including surveillance, doxxing, disinformation and threats from actors in the countries they fled. Thailand pledged, as a candidate for the UN Human Rights Council's 2025-2027 term, to develop policies and legislation protecting human rights in digital spaces. It must make that commitment meaningful for defenders at risk of transnational repression.



Lao activist Khieo Lapchanh, now missing in Thailand.
Before his disappearance on 15 September 2026, Khieo faced coordinated digital attacks, including violent AI-generated videos; his Facebook page had over 160,000 followers.

SOURCE: **Khiew Chennel** (Khieo's Facebook page) (20 March 2026)

Khieo: Online death threats before his disappearance in Thailand.

Khieo Lapchanh, a 26-year-old Lao activist living in Thailand, began speaking out about Laos on social media in December 2025. He subsequently faced coordinated online harassment, attempts to expose his whereabouts and an AI-generated video depicting him being beaten. In March 2026, an online commenter reportedly offered USD 8,000 to have Khieo killed and USD 2,000 to kill someone who defended him. Officials also visited his mother's home in Laos in connection with his activities. Khieo has been missing since leaving work in Samut Sakhon on 15 September 2026, the day before his first UNHCR interview. His whereabouts remain unknown. Whether his disappearance is connected to the threats has not been established; that possibility must be urgently investigated alongside all others. His case shows why digital transnational repression must be treated as a potential warning of physical danger.

This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

REALITIES ON THE GROUND

Challenges | **Case, Facts, and Comments**

Technology-facilitated Gender Based Violence (TFGBV)
Women human rights defenders, LGBTIQ+ activists and Indigenous rights advocates face overlapping risks: online harassment can expose their identities, undermine their credibility and intensify threats to their physical safety. Gendered attacks can include sexual intimidation, non-consensual sharing of intimate images and AI-generated abusive content.

Thailand's Penal Code Amendment Act (No. 30) B.E. 2568 (2025), which took effect on December 30, 2025, formally establishes sexual harassment as a distinct, standalone criminal offense
Thailand's new offence of sexual harassment, including online harassment, and its court-based "Take It Down" procedure are important advances. However, the removal procedure addresses content covered by the new provisions; compensation requires a separate process, and its effectiveness for survivors remains to be seen. These measures must be accompanied by effective protection against doxxing, coordinated attacks and cross-border threats, with accessible remedies for women and LGBTIQ+ defenders.

CEDAW General Recommendation 35 on gender-based violence. CEDAW General Recommendation 35 explicitly addresses gender-based violence against women in digital settings, requiring enforceable civil and criminal remedies, support services for survivors, and training for law enforcement.



Tanruthai "Pim" Thanrut: gendered digital repression against a young lesbian defender.
Pim is a young lesbian human rights defender, co-founder of youth democracy group Mokeluang Rimnam, campaigner for the #SaveBangKloi campaign in support of Bangkloi indigenous villagers, and Protection Associate at Manushya Foundation. After sharing her experience of sexual assault in a social media post, Pim was subjected to widespread abuse, including vulgar insults, victim-blaming, and harassment. By mid-2023, she was further targeted through the circulation of her photographs with sexually explicit threats and the receipt of unsolicited sexual imagery. Her experience reflects how intersecting identities (LGBTIQ+, survivor, youth activist, Indigenous advocate) compound exposure to online attacks.

Nada Chaiyajit: SLAPP criminal defamation case for legal representation and advocacy on trans woman's sexual harassment.
Nada is a prominent LGBTI leader, feminist human rights defender, the founder of Intersex Thailand and an academic. She was sued for defamation following her public advocacy exposing the sexual harassment of a transgender woman by a politician and business owner. The Court ultimately dismissed the case and recognised Nada's role as a human rights defender, marking an important legal precedent, but the proceedings imposed significant legal and psychological burdens.

Challenge 4: Online censorship, media regulation, platform coercion, identity verification and emerging age-gating proposals

Content removal and platform liability.
Thai authorities can direct platforms to remove certain content without first obtaining a court order. The 2022 Ministerial Decree on content takedown effective from December 2022 sets deadlines as short as 24 hours for some alleged offences under Section 14 of the Computer Crime Act (CCA). Failure to comply can create a presumption that a provider cooperated in, consented to or acquiesced in the offence, exposing it to liability under Section 15. Although affected users and providers can appeal to the Ministry of Digital Economy and Society (MDES), an appeal does not suspend the removal order. A separate rule, the 5 July 2025 Notification of the Electronic Transactions Commission on Measures to Prevent Technological Crimes for Social Media Service Providers, effective from July 2025 requires social media providers seeking protection from liability under the 2002 technological-crimes decree to remove specified allegedly false or misleading content within 24 hours of MDES notification. These short deadlines give platforms an incentive to remove content before its legality can be independently assessed

Meta 2025: over 11,400 items restricted following Thai government requests. In the first half of 2025, Meta restricted at least 1,400 items following requests linked to Section 112; in the second half, over 10,000 additional items were restricted, including 1,600 related to Section 112.

Google reported 118 removal requests between January and June 2025, following 266 in 2024 and 255 in 2023, with criticism of the government as the primary target.

YouTube and TikTok reported 100% compliance in 2023.
The 2023 Freedom on the Net vvreport revealed that YouTube and TikTok each complied with 100 per cent of Thai government content removal orders.

This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

REALITIES ON THE GROUND

Challenges | **Case, Facts, and Comments**

Media regulation and online journalism.

The Draft Media Ethics and Professional Standards Promotion Act, approved by the Cabinet on 11 January 2022, is a legislative proposal in Thailand aimed at establishing a national regulatory body to oversee journalism, media outlets, and online content creators.

It proposed a Media Professional Council to set ethical standards, handle complaints and oversee registration of professional media organisations. The draft also conditioned media freedom on broadly worded concepts including "public morals". Journalists raised concerns that such language and a state-funded oversight body could be used to pressure critical reporting, including journalism published online. Although the bill lapsed in 2023, a Senate subcommittee was tasked in April 2026 with studying it for future proposals. The risk is therefore renewed legislation based on the draft, rather than the imminent adoption of the lapsed bill.

Techno-colonialism and platform accountability.

US-based platforms enforce content rules in Thailand that may disregard Thai law and local needs. When lawful reproductive-health information is removed, feminist organisations can lose a vital way to reach people seeking care.

Identity verification and access to communication.

On 15 August 2025, the National Broadcasting and Telecommunications Commission (NBTC) announced the use of facial liveness detection for SIM registration. Implemented nationwide from 18 August 2025, the measure applies to new subscribers and existing subscribers replacing a SIM while retaining their number. In November 2025, the Ministry of Digital Economy and Society discussed further SIM-registration checks and stronger identity verification on online platforms. They proposed a **"Survival SIM"** arrangement that would limit SIM access for people listed as operators of mule accounts and require registration through the Department of Provincial Administration.

Separately, the Electronic Transactions Commission's Notification on Measures to Prevent Technological Crimes for Social Media Service Providers (No. 2) was published on 5 May 2026 and is due to take effect on 1 November 2026. It requires social media providers carrying paid advertisements in Thailand to verify advertisers' identities and retain specified information. It does not require identity verification for all social media users. These identification measures raise concerns about privacy and access to communication, particularly for people without accepted identity documents or those wrongly flagged as linked to mule accounts.

Emerging age-gating proposals.

On 9 September 2026, the Ministry of Digital Economy and Society (MDES) advocated age-assurance measures for young users and proposed regional standards for cross-platform user verification, with Thailand's Digital ID as a possible component. The Ministry confirmed that Thailand had not set a minimum age for social media use. Nevertheless, mandatory age or identity checks could restrict young people's access to information and online communities, particularly those who lack accepted documents, and could undermine privacy and anonymity.

Website blocking reaches political advocacy.

Thailand's Ministry of Digital Economy and Society reported blocking 45,024 URLs between October 2022 and December 2023, including 4,592 gambling-related URLs. Targets extend beyond legitimately restricted content to include political advocacy, social media, civic petition platforms, and tools for anonymity and circumvention, including VPNs (Ultrasurf, Anonymouse, Hotspot Shield). These measures can suppress political advocacy and restrict access to information while leaving users with limited visibility into why content or sites disappear.

Press Freedom Risks:

Draft Media Ethics and Professional Standards Promotion Act's broad and poorly defined provisions, such as protecting "public order" and "good morals", introduce severe risks of arbitrary interpretation, turning legitimate reporting into a target for state-sponsored censorship and digital surveillance. By imposing mandatory registration for content creators and establishing a state-funded council, the legislation dismantles the principle of independent media self-regulation and replaces it with centralized government oversight. This structural shift fundamentally threatens freedom of expression and press independence, as it creates an environment ripe for weaponizing administrative penalties against online dissent, suppressing investigative journalism, and restricting the public's right to access uncensored information.



The suppression of lawful reproductive-health information by Meta.

On 12 May 2025, feminist platform "Safe Abortion Thailand" Facebook Page, administered by **Tamtang Foundation** and providing information on legal abortion, was suspended, and was re-initiated after Manushya and partners wrote to Meta. On 19 May, another abortion rights page, **RSA Thai's** Facebook page was suspended, and reinstated the same day. It was suspended again on 26 May and reinstated the next day, following Manushya's intervention with Meta. By applying anti-feminist conservative, U.S.-centric moderation standards in a Thai context where abortion is legal, Meta is exporting digital patriarchy and undermining Thai sovereignty and law. This is a clear case of techno-colonialism, where foreign corporate policies override the rights and laws of Global South communities. The cases show why platforms must assess content in its local legal and human-rights context, provide meaningful appeals, and remedy wrongful removals promptly.

Age-gating is Anti-Poor.

Manushya opposes age-gating frameworks because they could restrict young people's access to information, expression and online communities, with disproportionate effects on working-class, racialised and migrant youth. Methods that collect identity documents or biometric information would also create privacy and anonymity risks. These are concerns about an emerging policy direction, rather than effects of a general age-gating law already in force.

This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

REALITIES ON THE GROUND

Challenges | **Case, Facts, and Comments**

Challenge 5: Absence of rights-respecting AI governance, gaps in data protection, and environmental and social harms of data centre expansion

Gaps in data protection. Thailand's Personal Data Protection Act (PDPA), enforced from June 2022, excludes certain operations of public authorities responsible for state security and public safety. Those authorities must still maintain prescribed data-security protections, but the exemption leaves a substantial gap in the law's other safeguards. The Personal Data Protection Committee also includes senior government officials, raising concerns about its independence when state data practices require scrutiny.

Data centres' environmental and community impacts.
AI growth is adding to demand for data centres, particularly in the Eastern Economic Corridor. In March 2026, Mongabay identified more than 70 data-centre projects in Thailand: approximately 40 operating, 20 under construction and 10 planned. Their water and electricity needs raise concerns in areas where communities and industry already compete for resources. Project assessments should disclose expected water use, electricity demand and effects on local livelihoods, and give affected communities a meaningful opportunity to participate.



The construction site of Bridge Data Centre's 0.2 GW QHI01 data centre in Khlong Tamru subdistrict, Chonburi province, Thailand.

SOURCE: Andy Ball/Mongabay (February 2026)

Thailand launched the AI-powered Cyborg 1.0 robot "AI police robot) to enhance 'security' at public gatherings. In April 2025, Nakhon Pathom police deployed AI Police Cyborg 1.0 during Songkran, one of Thailand's most significant cultural celebrations attended by millions of people including children, tourists, ethnic minorities, and members of the LGBTIQ+ community. Reported capabilities included facial recognition against police watchlist, tracking people through connected CCTV and drone footage, and detecting behaviour classified as violent or disruptive. These tools, framed as security measures, are weaponized to crush civic resistance. Facial recognition and behavioural surveillance technology deployed without legal basis, without disclosure of criteria for "blacklisted" individuals or "disruptive" behaviour, and without any mechanism for those surveilled to know they have been identified, tracked, or flagged, constituting a serious and unjustified interference with the right to privacy under Article 17 of the ICCPR.

UN Special Rapporteurs on FoE, AI moratorium.
The UN Special Rapporteurs on Freedom of Expression, Situation of Human Rights Defenders, Freedom of Peaceful Assembly and Association, and the UN Working Group on Business and Human Rights have called for an immediate moratorium on the sale and transfer of commercial surveillance tools such as Pegasus until rigorous human rights safeguards are in place, and have emphasised that the right to privacy includes the right to know who holds information and how it is used.

Chonburi data centre is projected to consume 3.3 million cubic metres of water per year, roughly equivalent to 37,000 residents. Data centres require enormous volumes of water for cooling systems: one planned facility alone is projected to require 3.3 million cubic metres of water annually, roughly equivalent to the annual water consumption of nearly 37,000 residents. This places technology corporations including Google and Microsoft in direct competition with local farmers and fishers for access to water sources under stress. Reservoir levels in Chonburi province are declining, and residents report fears that continued industrial development will leave communities without running water. Thailand's electricity grid relies on fossil fuels for approximately 85 per cent of generation capacity, meaning the increased electricity demand from data centre expansion also drives up carbon emissions and air pollution.

RECOMMENDATIONS

1. On Challenge 1: Repeal weaponised laws and decriminalise defamation

1.1	Repeal Section 112 of the Criminal Code to bring it into full conformity with Article 19 of the ICCPR, including by removing mandatory minimum sentences, eliminating the possibility of third-party complaints, and ensuring that no expression constituting legitimate political commentary, satire, or criticism of public institutions can give rise to criminal liability, in line with 3rd UPR recommendations 52.57, 52.60, 52.64 and Human Rights Committee General Comment 34.

This UPR Factsheet was prepared by **Manushya Foundation, GIRLxGIRL, Young Pride Foundation, Buriram Plod-Aek, Mokeluang Rimnam, Tamtang Foundation, Muslim Attorney Centre Foundation, Thai CSOs Coalition for the UPR and UN dsa, Civil Society Assembly for Peace, Prof. Haji Sulong Abdulqadir Tohmeena Foundation, Jaringan Mangsa Dari Undang-Undang Darurat (JASAD), Tanah Kita Foundation, The Hooman, The Patani, Patani Human Rights Organisation**

RECOMMENDATIONS

1.2	Repeal Section 116 of the Criminal Code to remove vague and overbroad provisions that permit the prosecution of individuals for peaceful political expression online or offline, in line with 3rd UPR recommendations 52.61 and 52.65.
1.3	Repeal the Computer Crimes Act (2017), including Sections 14 to 17, to ensure that its provisions comply with the requirements of legality, necessity and proportionality under international human rights law, in line with 3rd UPR recommendations 52.49, 52.62 and 52.65.
1.4	Decriminalise defamation entirely and remove criminal penalties under Sections 326 to 333 of the Criminal Code, replacing them with proportionate civil remedies, in line with 3rd UPR recommendation 52.46 and repeated calls in reports of the UN High Commissioner for Human Rights.
1.5	Immediately and unconditionally release all individuals detained solely for the peaceful exercise of their right to freedom of expression online or offline, including those in pretrial detention on Section 112 charges, and drop all pending charges against them. Implement the August 2024 UN Working Group on Arbitrary Detention determination on the detention of Arnon Nampa, including his immediate release and enforceable reparations.

2. On Challenge 2: End Pegasus spyware, information operations, and AI-equipped surveillance of minorities,

2.1	Immediately cease the use of Pegasus spyware and all other commercial surveillance tools against activists, journalists, human rights defenders, political opponents and civil society organisations; conduct an independent and transparent investigation into all confirmed and alleged uses of such tools; provide effective remedies including reparations to those whose devices were infected; and publish the results of any investigation, in line with the UN Special Rapporteur on Freedom of Expression's 2019 report on surveillance and human rights, which called on states to impose an immediate moratorium on the sale and use of surveillance technology until adequate human rights safeguards are in place.
2.2	Support and implement the call by the UN Special Rapporteurs on Freedom of Expression, Situation of Human Rights Defenders, Freedom of Peaceful Assembly and Association, and the UN Working Group on Business and Human Rights for a global moratorium on the sale and transfer of commercial surveillance technology until rigorous human-rights safeguards are in place. Pending those safeguards, halt Thailand's procurement and import of such tools.
2.3	Ensure that international technology platforms operating in Thailand publicly and independently review data disclosure practices, given Meta's reported 84.47% compliance rate with Thai state data requests in the first half of 2025 (3,452 requests covering 6,045 users and accounts), and that any disclosure complies with international human rights standards on legality, necessity and proportionality.
2.4	Disband the Cyber Team operating under the Joint Command Center of the Internal Security Operations Command (ISOC), and any other State unit engaged in coordinated online harassment, cyberattacks, or information operations targeting civil society organisations, human rights defenders, journalists or political opponents, and ensure those responsible are held accountable through independent judicial proceedings.

For more information, evidence and data, please refer to the References and/or contact:
Jean Linis-Dinco, Manushya Foundation. Email: jean@manushyafoundation.org

RECOMMENDATIONS

2.5	Immediately cease the deployment of the 8,200+ AI-equipped surveillance cameras in the Deep South provinces of Yala, Pattani, Narathiwat and Songkhla districts used to monitor ethnic Malay Muslim communities, and suspend the collection of biometric data from children and community members without adequate legal basis, consent, or independent oversight, in line with the UN Special Rapporteur on Minority Issues' guidance on the rights of ethnic and religious minorities.

3. On Challenge 3: Address digital transnational repression and technology-facilitated gender-based violence

3.1	Investigate and prevent cross-border online harassment campaigns against dissidents residing in Thailand, including the coordinated attacks against "Khieo" that included USD 8,000 and USD 2,000 bounties on his life and that of a supporter, and address the emerging threat of AI-generated deepfakes and simulated violence used to escalate harassment into offline harm.
3.2	Cease all acts of transnational repression against Thai dissidents and activists living abroad, and against foreign dissidents residing in Thailand, including surveillance and coordination with foreign governments for the purposes of targeting individuals for their online expression, in line with the UN Special Rapporteur on Human Rights Defenders' 2022 report on transnational repression. Ensure protection of Lao, Cambodian, Vietnamese, Burmese, Chinese and other dissidents residing in Thailand from cross-border digital repression by their home governments.
3.3	Adopt comprehensive legislation specifically addressing technology-facilitated gender-based violence (TFGBV), including doxxing, non-consensual sharing of intimate images, and coordinated online harassment campaigns, with enforceable civil and criminal remedies, support services for survivors, and training for law enforcement, in line with CEDAW General Recommendation 35 on gender-based violence against women.
3.4	Ensure that all TFGBV legislation and enforcement practices explicitly protect women human rights defenders, LGBTIQ+ activists, Indigenous rights advocates, and other defenders facing intersectional online attacks, and provide gender-responsive investigation and remedies for cases.
3.5	Ensure that criminal defamation and CCA provisions are not weaponised against women and LGBTIQ+ defenders, journalists and academics exposing gender-based violence and workplace abuse.
3.6	Establish adequate protection and rapid response mechanisms for women, LGBTIQ+, Indigenous and youth defenders subjected to sustained gender-based digital repression, with dedicated resources and cross-border cooperation to counter transnational patterns of attack.

SCAN HERE

Scan to access the **Joint UPR submission on Digital Rights**

For more information, evidence and data, please refer to the References and/or contact:
Jean Linis-Dinco, Manushya Foundation. Email: jean@manushyafoundation.org

RECOMMENDATIONS

4. On Challenge 4: End extrajudicial content removal, platform coercion, and mandatory identity verification

4.1 Repeal the 2022 Ministerial Decree on content takedown and the 5 July 2025 Notification of the Electronic Transactions Commission on Measures to Prevent Technological Crimes for Social Media Service Providers to ensure that content removal obligations comply with the three-part test of legality, necessity and proportionality under Article 19(3) of the ICCPR, require judicial authorisation for removal orders, provide for meaningful appeal mechanisms, and prohibit joint liability on platforms for content they have not been formally ordered to remove.

4.2 Ensure that the Draft Media Ethics and Professional Standards Promotion Act is not adopted in its current form, given that its mandatory registration requirements, vague ethical standards, and potential for licence revocation on grounds of non-compliance with "public morals" are incompatible with the right to freedom of expression and press freedom under Article 19 of the ICCPR and the standards set out by the Special Rapporteur on Freedom of Expression regarding the regulation of media.

4.3 Withdraw the National Broadcasting and Telecommunications Commission's August 2025 SIM-registration measure requiring facial liveness detection, because it risks disproportionately restricting access to mobile communications for marginalised communities, including LGBTIQ+ youth, migrants and dissidents.

4.4 Revise advertiser identity-verification requirements to protect access to communication. Amend the Electronic Transactions Commission's Notification on Measures to Prevent Technological Crimes for Social Media Service Providers (No. 2) to limit verification and data collection to what is necessary for paid advertising, provide workable alternatives for advertisers without standard identity documents, and set clear limits on access to and retention of their data. Do not extend mandatory identity verification to all social media users.

4.5 Cease the mass URL blocking practices documented since 2022 (from 4,735 URLs in 2022 to 45,024 URLs between October 2022 and December 2023) that extend well beyond legitimately restricted content to include political advocacy, civic petition platforms, and tools for anonymity and circumvention.

4.6 Ensure that content moderation frameworks applied by international platforms operating in Thailand account for local legal contexts and do not restrict access to lawful, life-saving information, addressing the recurring suppression of feminist pages.

4.7 Ensure Non-Discriminatory Content Moderation and Mandate Transparency from Tech Companies by developing binding national guidelines, through consultation with affected communities, to ensure that platforms' content moderation policies do not disproportionately target LBTIQ+ users, sex workers, or abortion rights defenders. Require all platforms operating in Thailand to disclose content governance practices, algorithmic decision-making, and anonymized data disaggregated by gender, SOGIESC, and advocacy topic (e.g., abortion, sex work, LGBTIQ+ rights). Ensure that content moderation frameworks applied by international platforms operating in Thailand account for local legal contexts and do not restrict access to lawful, life-saving information, addressing the recurring suppression of feminist pages.

4.8 Refrain from introducing mandatory age-gating, minimum-age bans or cross-platform identity verification linked to Thailand's Digital ID as conditions for accessing social media; instead, require platforms to adopt privacy-protective child safety measures developed in meaningful consultation with children and young people, including those from marginalised communities.

For more information, evidence and data, please refer to the References and/or contact:
Jean Linis-Dinco, Manushya Foundation. Email: jean@manushyafoundation.org

RECOMMENDATIONS

5. On Challenge 5: Adopt rights-respecting AI governance, close data protection gaps, and address data centre harms

5.1 Amend the Personal Data Protection Act to remove the broad exemption for public authorities with national security responsibilities, ensure that State surveillance activities are subject to meaningful data protection obligations, and establish an independent Personal Data Protection Committee with genuine autonomy from government, in line with 3rd UPR recommendation 51.93 and the standards of the UN Special Rapporteur on the Right to Privacy.

5.2 Reject the proposed "risk-based" approach to AI governance as incompatible with the inalienable, non-derogable character of fundamental human rights, and develop and adopt a legally binding, rights-respecting, tech-agnostic regulatory framework that includes mandatory human rights impact assessments prior to the deployment of technological systems in public sector contexts, enforceable legal remedies for individuals harmed by algorithmic decision-making, and a prohibition on the deployment of AI-powered surveillance tools against civil society without independent judicial authorisation.

5.3 Immediately halt the deployment of AI-powered surveillance in public and cultural contexts, and prohibit facial recognition and behavioural surveillance technology in public spaces without legal basis, public disclosure of criteria, and mechanisms for those surveilled to know they have been identified.

5.4 Ensure meaningful participation of affected communities in the planning and approval of data centre projects. Halt data centre projects that lack genuine consultation with affected communities, and adopt binding standards on water use, energy sources, carbon emissions, and community impact, given projected water consumption of up to 3.3 million cubic metres per facility per year and Thailand's 85 per cent fossil fuel electricity generation.

5.5 Ratify and implement without reservations the international human rights obligations of the ICCPR, ICESCR and other treaties in the digital and AI context, and cooperate with the mandates of the UN Special Rapporteurs on Freedom of Expression, the Right to Privacy, the Right to Health, Minority Issues, the Situation of Human Rights Defenders, and Freedom of Peaceful Assembly and Association in the design and monitoring of digital and AI regulation.

SCAN HERE

Scan to access the **Joint UPR submission on Digital Rights**

For more information, evidence and data, please refer to the References and/or contact:
Jean Linis-Dinco, Manushya Foundation. Email: jean@manushyafoundation.org

NOTES