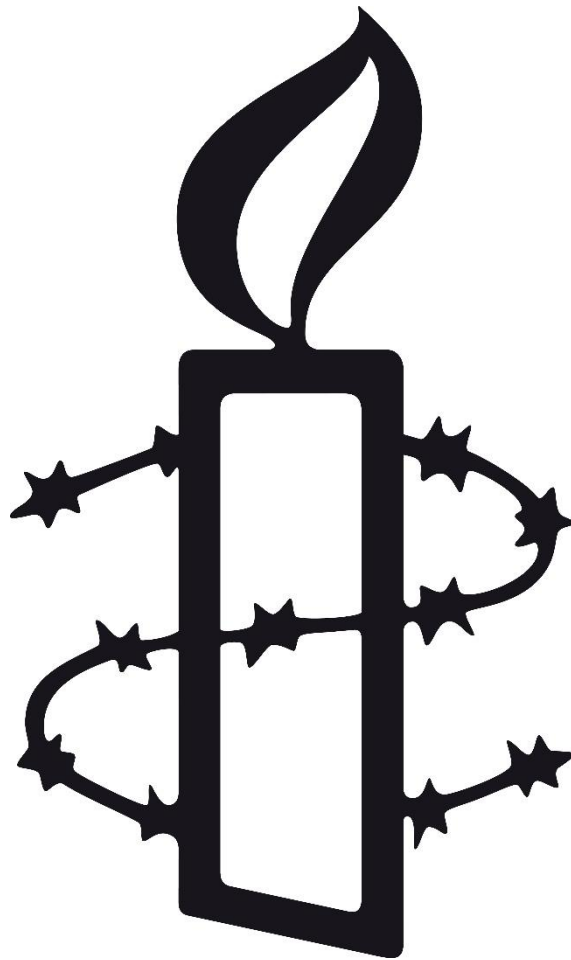


THAILAND

SUBMISSION TO THE UN COMMITTEE ON THE ELIMINATION OF
DISCRIMINATION AGAINST WOMEN, 91ST SESSION, 19 JUNE 2025



CONTENTS

1. INTRODUCTION	3
2. TFGBV AGAINST HUMAN RIGHTS DEFEDERS (ARTICLES 2, 5, AND 7)	3
2.1. Targeted digital surveillance and gendered impacts	3
2.2. Online harassment	5
2.3. The chilling effect	7
2.4. Lack of access to justice for survivors	7
3. CONCLUSION AND RECOMMENDATIONS	8

Amnesty International provides the below information to the UN Committee on the Elimination of Discrimination Against Women (“The Committee”) ahead of the review of Thailand’s eighth periodic report as a State Party to the Convention on the Elimination of All Forms of Discrimination against Women (“CEDAW”) on 19 June 2025. It reflects Amnesty International’s key concerns about technology-facilitated gender-based violence (TfGBV) against women and gender-diverse human rights defenders (HRDs).

1. INTRODUCTION

Amnesty International provides the below information to the UN Committee on the Elimination of Discrimination Against Women (“the Committee”) ahead of the review of Thailand’s eighth periodic report as a State Party to the Convention on the Elimination of All Forms of Discrimination against Women (“CEDAW”) in June 2025.

This submission reflects Thailand’s failure to meet its obligation under CEDAW and other international human rights instruments to guarantee the right to be free from violence, including gender-based violence (GBV), in the digital space. It focuses on Amnesty International’s key concerns about technology-facilitated gender-based violence (TfGBV) against women and gender-diverse human rights defenders (HRDs).

The submission is primarily based on Amnesty International’s own research, as well as secondary news reports, court records, legal and policy documents.

1. TFGBV AGAINST HUMAN RIGHTS DEFEDERS (ARTICLES 2, 5, AND 7)

In the last Concluding Observations, the Committee raised alarms that “women human rights defenders, in particular those advocating for land rights, protection of the environment and the rights of indigenous women, rural women, lesbian women, bisexual women, transgender women and Muslim women in the southern border provinces, have increasingly become targets of lawsuits, harassment, violence and intimidation by authorities and business enterprises because of their work.”¹

During the period under review, the Committee’s concerns remain relevant as women and gender-diverse human rights defenders (HRDs) continue to be targeted because of their work. Between 2020 and 2024, Amnesty International’s research documented 40 emblematic cases, where women, girls and other gender-diverse HRDs faced TfGBV in reaction to their human rights activism.²

Amnesty International’s research identified the two key forms of TfGBV in Thailand: targeted digital surveillance and online harassment.

2.1. TARGETED DIGITAL SURVEILLANCE AND GENDERED IMPACTS

Between 2020 and 2022, dozens of women, girls and gender-diverse HRDs in Thailand experienced targeted digital surveillance - a practice of monitoring or spying on specific persons and/or organizations, through digital technology, to interfere with their private data.³ Amnesty International documented the use of Pegasus spyware against cisgender women HRDs and attacks on individual Facebook accounts against both women and gender diverse HRDs.

¹ UN Committee on the Elimination of Discrimination Against Women (“CEDAW Committee”), Concluding observations of the Committee on the Elimination of Discrimination against Women on the combined sixth and seventh periodic reports of Thailand, 24 July 2017, UN Index: CEDAW/C/THA/CO/6-7, para 30.

² Amnesty International, “Being ourselves is too dangerous”: Digital violence and the silencing of women and LGBTI activists in Thailand, Index: ASA39/7955/2024, 16 May 2024, <https://www.amnesty.org/en/documents/asa39/7955/2024/en/>.

³ Amnesty International, *Ending the Targeted Digital Surveillance of Those Who Defend Our Rights* (Index: ACT 30/1385/2019), 20 December 2019, <https://www.amnesty.org/en/documents/act30/1385/2019/en/>, p. 4.

The use of Pegasus spyware

In 2022, Citizen Lab, together with iLaw and Digital Reach, published forensic research revealing that the devices of 35 individuals in Thailand were infected with Pegasus spyware developed by the Israel-based company NSO Group. Pegasus spyware allows unlimited access to the device and sends the information to another unauthorized entity without permission of the owner or operator, leaving little to no trace, so that the owner or operator of the device has almost no information as to what data was taken.⁴

The attacks took place between October 2020 and November 2021, during the height of the youth-led pro-democracy protest movement that started in mid-2020.⁵ The 35 individuals infected with the spyware comprised 15 women, 15 men and five anonymous individuals.⁶ All of them had publicly criticized the government, engaged in peaceful pro-democracy demonstrations and/or worked to defend the human rights of protesters.

Based on analysis of technical and circumstantial evidence, Amnesty International concluded there is a strong likelihood that one or more Thai state actors, or agents acting on their behalf, were involved in the use of the spyware. Evidence included the Thai government's history of targeting individuals whose phones were infected with the spyware, findings of technical investigations that identified the presence of Pegasus servers and operator in Thailand and the NSO Group's own policy that it exclusively sells its product to government agencies.⁷

Attacks on individual Facebook accounts

On 17 November 2022, at least 44 HRDs and environmental justice defenders reported having received a notification from Meta of "government-backed or sophisticated attacker alerts" via their personal Facebook accounts' support inbox.⁸ Of the 44 individuals, 18 are women and at least four are openly gender-diverse individuals.

Meta's Help Center indicated that this alert often targets civil society actors, including activists and outspoken critics, "to learn more about their activity online and offline and manipulate them into compromising their devices and online accounts".⁹

Unlike the case of Pegasus spyware, these 44 targeted individuals were not able to access sufficient information to determine the actor(s) behind these attacks.

Targeted digital surveillance as a form of gender-based violence

Amnesty International assesses targeted digital surveillance can be constitutive of gender-based violence prohibited under CEDAW because it leads to distinct gendered impacts, including fears of breach of privacy and bodily autonomy.

Many women HRDs reported suffering fear and anxiety that their private data could be used for sexualized blackmailing through the dissemination of their private data obtained through targeted surveillance to discourage them from carrying out further activism.¹⁰ Such gendered fear documented by Amnesty International is closely intertwined with the reality of gender-based violence in Thailand, where online violence against women, girls and gender-diverse people remains prevalent. The UN Working Group on Discrimination against Women and Girls emphasized in its end-of-mission statement

⁴ Citizen Lab, *GeckoSpy Pegasus Spyware Used against Thailand's Pro-Democracy Movement*, 17 July 2022, <https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement>.

⁵ Citizen Lab, *GeckoSpy Pegasus Spyware Used against Thailand's Pro-Democracy Movement* (previously cited).

⁶ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 43.

⁷ See the full details of Amnesty International's evidence at Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 48-49.

⁸ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 49.

⁹ Meta, "Facebook Help Center: Government-backed or sophisticated attacker alerts", <https://www.facebook.com/help/1550813285316567> (accessed on 10 January 2024).

¹⁰ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 52-53.

after an official visit to Thailand in December 2024, that “[m]any women and girls face online sexual harassment, cyberbullying, image-based abuse, and doxing, among other forms.”¹¹

2.2. ONLINE HARASSMENT

Amnesty International found that state and non-state actors have routinely weaponized online spaces to attack, intimidate and discredit women and gender-diverse HRDs, at least since the 2014 military coup.¹² The four common methods of online harassment included: doxing, the use of hateful and abusive speech, targeted smear campaigns and threats of gendered violence. These forms of online harassment are not mutually exclusive, and targeted HRDs often experienced several simultaneously.

Doxing

Malicious unidentified actors have used doxing against numerous women, girls and gender-diverse activists as a tactic of public shaming and intimidation.¹³

In one case, after a 17-year-old non-binary feminist HRD participated in various feminist protests, an anonymous account posted on X the HRD’s personal information, with details including their ID card numbers, full names and criminal charges against them, as well as a diagram illustrating their involvement in different protest actions.¹⁴ The post was published in August 2021 and remains active on the platform as of the submission date. The HRD told Amnesty International that this act of doxing created a strong sense of fear that their personal data would further be abused, especially because it happened when they were a child.¹⁵

Use of hateful and abusive speech

Women and gender-diverse HRDs who used social media platforms as an avenue for their human rights campaigning faced verbal attacks laced with misogynistic, homophobic and transphobic language.

Amnesty International documented organized harassment by means of cyber-mobbing, where a group of people staged a coordinated online attack against feminist groups and organizations. These malicious actors filled the comment sections with homophobic, transphobic and misogynistic language and prevented the public audience from engaging with feminism-related content online.¹⁶

Threats of violence

Many women and LGBTI HRDs received threats of violence through social media platforms both by means of public posts and comments and by private, direct messages.

In one example, in June 2022, three Muslim transgender women HRDs gave a media interview for an online news outlet about anti-LGBTI discrimination within the Muslim communities in Thailand. They later received a series of threats of violence from individuals who disagreed with their advocacy on

¹¹ UN Working Group on discrimination against women and girls, End of mission statement, Official visit to Thailand (2-13 December 2024), <https://www.ohchr.org/sites/default/files/documents/issues/women/wgdawg/statements/2024-12-13-eom-thailand-wgdawg-en.pdf>, p. 5.

¹² Amnesty International, “Being ourselves is too dangerous” (previously cited), p. 54.

¹³ Amnesty International, “Being ourselves is too dangerous” (previously cited), p. 65.

¹⁴ Amnesty International, “Being ourselves is too dangerous” (previously cited), p. 66.

¹⁵ Amnesty International, “Being ourselves is too dangerous” (previously cited), p. 67.

¹⁶ Amnesty International, “Being ourselves is too dangerous” (previously cited), p. 58-59.

gender equality for religious reasons.¹⁷ They received direct messages from individuals threatening to take their lives, hurt them or sexually assault them.¹⁸

Targeted smear campaigns against women and gender-diverse HRDs

Prominent women and gender-diverse HRDs were subjected to targeted smear campaigns. Such campaigns sought to delegitimize their activism through spreading gendered disinformation and negative narratives about the HRDs' lives to destroy their reputations and delegitimize their activism.¹⁹

State actors played a prominent role in orchestrating targeted smear campaigns against HRDs. In October 2020, X issued a statement that it uncovered a network of "information operations" linked to the Royal Thai Army (RTA) to target political opposition figures.²⁰ In February 2021, Meta's Coordinated Inauthentic Behavior report further confirmed that Thailand's Internal Security Operations Command (ISOC) had led an online operation that targeted Amnesty International among other civil society organizations and activists.²¹

One of the most well-known outlets for targeted smear campaigns against HRDs is the website 'pulony.blogspot.com' ("Pulony website"). During a parliamentary session in February 2020, a member of the Thai parliament revealed an official document by the Internal Security Operations Command (ISOC), which is the political wing of the Thai military.²² The website contained many articles that spread disinformation by portraying women HRDs working on peace and human rights in the conflict-plagued southern border provinces (SBPs) as part of the armed insurgent groups.²³

Women and gender-diverse HRDs working on civil and political rights have also fallen target to the smear campaigns. This included Amnesty International Thailand's former woman executive director.²⁴ The smear campaigns consistently spread disinformation that she worked as a foreign agent trying to undermine the Thai government. She also got attacked by sexualized slurs that are degrading or intimidating against women.²⁵

During a parliamentary debate on 25 March 2025, a parliamentarian disclosed leaked internal documents of a Cyber Team under a Joint Command Center run by police and military units, including those from the ISOC.²⁶ The Cyber Team's mission is to disseminate harmful and defamatory content online to tarnish the reputations of civil society organizations and political opposition members.

The documents indicated the Cyber Team also engaged in phishing attacks and brute-force attempts to access social media accounts. During the 2023 election period, it targeted the social media accounts of prominent activists, including Amnesty International Thailand's former woman executive director, through attempted brute-force attacks.²⁷

In response to these allegations, during the parliamentary debate, a representative of the Thai government categorically denied any involvement in a campaign of digital attacks.

¹⁷ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 68.

¹⁸ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 68.

¹⁹ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 59-65.

²⁰ X, "Disclosing networks to our state-linked information operations archive", 8 October 2020, https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information.

²¹ Meta, "February 2021 Coordinated Inauthentic Behavior Report", February 2021, <https://about.fb.com/wp-content/uploads/2021/03/February-2021-CIB-Report.pdf>, p. 5-8.

²² Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 59.

²³ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 60-62.

²⁴ Amnesty International Thailand's former woman executive director has left her position since 31 March 2025.

²⁵ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 65.

²⁶ Amnesty International, Thailand: Authorities must end malicious smear campaigns and cyberattacks on civil society, 7 April 2025, <https://www.amnesty.org/en/latest/news/2025/04/thailand-authorities-must-end-malicious-smear-campaigns-and-cyberattacks-on-civil-society/>

²⁷ Amnesty International, Thailand: Authorities must end malicious smear campaigns and cyberattacks on civil society (previously cited).

2.3 THE CHILLING EFFECT

Amnesty International documented that women and gender-diverse HRDs targeted with TfGBV suffered from severe mental impacts, including depression and post-traumatic stress disorder. Due to such negative impacts, the HRDs limited themselves online or disengaged from activism.

Gender-diverse HRDs in Thailand's Malay Muslim-majority SBPs strongly experienced the chilling effect that blocked them from publicly expressing themselves or undertaking activism in the digital space.²⁸ This chilling effect is connected to the severe discrimination and violence, including corporeal punishments, faced by gender-diverse people in the region due to their sexual orientation and gender identity.²⁹

2.4 LACK OF ACCESS TO JUSTICE FOR SURVIVORS

Lack of gender sensitivity in the police process

Women and gender-diverse activists told Amnesty International that they experienced unresponsive attitude of the police towards TfGBV. Many police officers did not take their complaints about TfGBV seriously and/or lacked understanding about the issue, which led to failures to register complaints, as well as distrust in law enforcement authorities among TfGBV survivors.³⁰

Challenges in the judicial system

The judicial system failed to deliver justice and redress for targeted women and gender-diverse HRDs. Due to various compounding factors, including the government's public denial of involvement in the spyware attacks and smear campaigns, the covert nature of the global spyware industry and the anonymity that is often linked to TfGBV, survivors struggle to obtain information about their perpetrators.³¹ Under Thai law, the burden of proof lies with the claimant in both criminal and civil lawsuits.³² Amnesty International found that this procedural requirement poses challenges for the survivors of TfGBV to access justice and redress through judicial mechanisms.³³

In November 2020, two prominent woman HRDs targeted with smear campaigns online – filed a lawsuit against the Office of the Prime Minister, which oversees the ISOC, and the RTA to the Bangkok Civil Court.³⁴ Both women HRDs alleged that these entities engaged in an online smear campaign. Due to the excessively high evidentiary threshold, the Bangkok Civil Court, on 16 February 2023, dismissed the case on the grounds that the plaintiffs did not have sufficient evidence to prove that the smear campaigns were run by the Thai state agencies on trial.³⁵

Gaps in the Gender Equality Act

There is no specific legislation protecting individuals against TfGBV, including gender-based online harassment, doxing and image-based abuse. The existing Computer Crimes Act contains broad provisions that do not align with international law and standards on the rights to freedom of expression and privacy.³⁶

²⁸ Amnesty International, "Thailand: Submission to the UN Committee against Torture, 81st Session, 28 October – 22 November 2024" (Index: ASA 39/8577/2024), 1 October 2024, <https://www.amnesty.org/en/documents/asa39/8577/2024/en/>, p.19.

²⁹ Amnesty International, "Thailand: Submission to the UN Committee against Torture, 81st Session, 28 October – 22 November 2024" (previously cited).

³⁰ Amnesty International, "Being ourselves is too dangerous" (previously cited), p 72-73.

³¹ Amnesty International, "Being ourselves is too dangerous" (previously cited).

³² Amnesty International, "Being ourselves is too dangerous" (previously cited).

³³ Amnesty International, "Being ourselves is too dangerous" (previously cited).

³⁴ Amnesty International, "Being ourselves is too dangerous" (previously cited), p. 74.

³⁵ Amnesty International, "Being ourselves is too dangerous" (previously cited).

³⁶ Amnesty International, Thailand: Grave concern over Thai Computer Crimes Act, (Index: ASA 39/4944/2016), 7 October 2016, <https://www.amnesty.org/en/documents/asa39/4944/2016/en/>

Gender-based discrimination, including discrimination on the basis of sexual orientation, sexual characteristics, and gender identity, is illegal in Thailand under the 2015 Gender Equality Act (GEA). The GEA set up the Committee on the Determination of Unfair Gender Discrimination (CDUGD) tasked to investigate complaints of gender-based discrimination and issue orders for state or non-state entities to cease and prevent discriminatory acts and provide compensation for survivors of such acts.³⁷

While the CDUGD could have been a useful mechanism for addressing TfGBV. However, Section 17(2) of the GEA allows for exemptions in cases where such discriminatory acts are carried out “for following religious practices, or for security of the nation”.³⁸ The CDUGD is therefore unable to take up cases falling under this exemption.³⁹ With such limitations, none of the perpetrators who committed TfGBV, including cases where state actors were suspected to be involved, could be brought before this mechanism.

During the previous review, the Committee raised concerns around these exemptions provided under Section 17(2) of the GEA and provided recommendations to lift these exemptions.⁴⁰ However, the government has not followed this recommendation. Thailand also has not yet adopted comprehensive anti-discrimination legislation which protects individuals from other forms of discrimination, for example, on grounds of colour, descent, national origin, religion or socio-economic status.⁴¹

3. CONCLUSION AND RECOMMENDATIONS

Amnesty International concludes that the Thai government has failed to meet its obligations to refrain from engaging in TfGBV and prevent, investigate, prosecute, punish and provide reparations for acts or omissions by both state and non-State actors in line with the Convention.

To address the issue of TfGBV, Amnesty International recommends that Thailand:

1. Take the following actions to protect women and gender-diverse people:

- Publicly commit to refraining from the use of TfGBV, and to protect HRDs and other members of civil society from such violence
- Carry out a prompt, independent, impartial and transparent investigation into all documented and reported instances of TfGBV against women and gender-diverse HRDs
- Proactively remove structural and systemic barriers to gender equality, including by undertaking legislative measures, social policies and educational programmes to eliminate gender and other intersectional harmful stereotypes, negative social norms and discriminatory attitudes against women, girls and gender-diverse people, with specific attention to the situation of LGBTI people in the SBPs
- Establish and enforce codes of conduct on public communications for officials to ensure state actors do not engage in online harassment, including the use of gendered disinformation, against women and gender-diverse HRDs

³⁷ Thailand, Gender Equality Act (2015), <https://www.ratchakitcha.soc.go.th/DATA/PDF/2558/A/018/17.PDF>, Sections 14 and 20.

³⁸ Thailand, Gender Equality Act (2015) (previously cited), Sections 17.

³⁹ Amnesty International, “Being ourselves is too dangerous” (previously cited), p 35.

⁴⁰ CEDAW Committee, Concluding observations of the Committee on the Elimination of Discrimination against Women on the combined sixth and seventh periodic reports of Thailand (previously cited), para 9.

⁴¹ Amnesty International, “Being ourselves is too dangerous” (previously cited), p. 36.

2. Prevent further targeted digital surveillance against women and gender-diverse HRDs
 - Proactively disclose information about all previous, current and future contracts between all state entities, including security agencies, and private surveillance companies
 - Enforce a ban on highly invasive spyware, whose functionality cannot be limited to only those functions that are necessary and proportionate to a specific use and target, or whose use cannot be independently audited
 - Implement a human rights regulatory framework that governs surveillance and is in line with IHRL and standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer and use of all surveillance technologies should be enforced
3. Carry out the following legal reforms:
 - Enact and implement comprehensive legislation to recognize, prevent, document, investigate and prosecute TfGBV and provide redress and support for survivors
 - Amend the 2015 Gender Equality Act by removing exemptions that gender-based discrimination on grounds of religious principles and national security are permissible under Section 17(2) of the law, in line with the recommendation from the CEDAW Committee
4. Instruct law enforcement agencies to take the following actions:
 - Prioritize capacity-building and training of all law enforcement bodies on TfGBV and guarantee survivors' access to justice in line with international human rights law and standards
 - Adopt a specialized protocol for law enforcement officials in addressing TfGBV through a gender-sensitive, trauma-informed response
 - Provide protection for women and gender-diverse HRDs who wish to pursue legal actions for TfGBV to ensure they are safe from reprisals

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Contact



info@amnesty.org



facebook.com/
AmnestyGlobal



@Amnesty



amnesty.org



Amnesty International
Peter Benenson House
1 Easton Street
London WC1X 0DW, UK

Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence (see creativecommons.org/licenses/by-nc-nd/4.0/legalcode).

Where material is attributed to a copyright owner other than Amnesty International, this material is not covered by the Creative Commons licence.

For more information, visit the [permissions page](#) on Amnesty International's website.

Index: ASA 39/9361/2025

Publication: May 2025

Original language: English

© Amnesty International 2024