



# “BEING OURSELVES IS TOO DANGEROUS”

DIGITAL VIOLENCE AND THE SILENCING OF WOMEN AND LGBTI HUMAN RIGHTS DEFENDERS IN THAILAND

**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.**

© Amnesty International 2024

Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

For more information please visit the permissions page on our website: [www.amnesty.org](http://www.amnesty.org)

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

First published in 2024

by Amnesty International Ltd

Peter Benenson House, 1 Easton Street

London WC1X 0DW, UK

Index: ASA 39/7956/2024

Original language: English

[amnesty.org](http://amnesty.org)



Cover illustration: © Summer Panadd

**AMNESTY**  
INTERNATIONAL



# EXECUTIVE SUMMARY

***Content warning: This report contains descriptions of violence and abuse against women and LGBTI people.***

In November 2021, Niraphorn Onnkhaow, a 22-year-old university student and one of the organizers of the youth-led pro-democracy protest group United Front of Thammasat and Demonstration (UFTD), received an e-mail from Apple alerting her that “[s]tate-sponsored attackers may be targeting your iPhone”. A few

months later, she found out through civil society-led forensic research that she was among 35 human rights defenders (HRDs), activists, academics and artists, including 15 women, targeted with Pegasus, a highly invasive spyware developed by the Israeli cyber intelligence company NSO Group. Her device was infected 14 times in 2021 – the highest number of infections among all the targeted individuals.

The spyware infections came as a shock for Niraphorn Onnkhaow, who had no public-facing role in her activism. “I was extremely shocked and terrified when I learned that I was targeted. I’ve already tried to mitigate my risks by only working on back-end operations... Keeping a low profile could not protect me,” she told Amnesty International. Only a few months before finding out about the spyware infection, a Facebook page had posted her personal information online to expose her role in the UFTD, which was not public information at that time.

As a result of these digital attacks, she decided to end her role in the protest movement due to fears that her private data could be weaponized against her if she continued being involved in protests. “As a woman, having my privacy invaded is frightening... If I have private photos on my phone, they could be leaked to smear my reputation and hurt me to the extent that I’d have to stop my activism. The impacts of such blackmailing won’t be the same for men because women tend to be penalized more for this type of scandal in the Thai society,” she explained to Amnesty International.

Niraphorn Onnkhaow’s experience is emblematic of the targeted use of technology-facilitated gender-based violence (TfGBV) designed to silence women and LGBTI HRDs in Thailand. TfGBV is any act of violence, or threats thereof, perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, that disproportionately impacts women, girls and other people based on their real and/or perceived sexual orientation, gender identity and/or expression, causing physical, psychological, economic and sexual harm. Gender-based violence exists in a continuum between physical and digital spaces.

Amid intensifying state repression of the offline civic space after the Thai military staged a coup and took power in May 2014, and the emergence of the youth-led pro-democracy movement in 2020, digital technology has become a vital tool for women and LGBTI people to carry out activism and raise awareness about human rights. Nonetheless, the digital space is not always safe for women and LGBTI HRDs, exposing them to gender-based violence.

Thailand has long positioned itself as a champion of gender equality. The Tourism Authority of Thailand’s campaign “Go Thai, Be Free” presents Thailand as the “most LGBTIQ / LGBTI+ welcoming country in Asia” and states that: “In Thailand, we believe diversity is amazing”. In 2022, Thailand hosted the Global Summit of Women where the former Prime Minister, Prayut Chan-o-cha, pledged to promote gender equality and empower women. In 2023 a new government similarly expressed its commitment to guarantee “gender equality” and pledged to pass laws to legalize same-sex marriage, decriminalize sex work and allow for legal gender recognition with an ambitious goal for Thailand to become the host of World Pride in 2028.

This report, however, presents a stark contrast between the government’s official commitment to gender equality and the lived reality of women and LGBTI HRDs who have had to suffer from TfGBV as a result of

their activism. As part of Amnesty International's global campaign Protect the Protest, the report provides an in-depth analysis of different forms of TfGBV and its harmful impact on women and LGBTI HRDs. Ultimately, TfGBV in Thailand has resulted in a chilling effect, deterring women and LGBTI people from fully expressing themselves or their opinions and engaging in activism. As the testimonies in this report show, TfGBV and offline violence against women and LGBTI people function in an intricate interplay where they often mirror, exacerbate and amplify each other.

Amnesty International conducted group and individual interviews with 40 HRDs, including 14 cisgender heterosexual women and 26 LGBTI people. At least 25 of the interviewees were youths under 25 years old at the time they experienced TfGBV, including two HRDs who were under 18. Many interviewees were also Malay Muslims from the country's southern border provinces (SBPs), where negative attitudes towards women and LGBTI people remain prevalent.

To corroborate information received from the interviewees, Amnesty International carried out extensive desk research through analysis of content on social media platforms. This research method was selected to avoid asking interviewees to revisit past incidents of TfGBV that can result in re-traumatization.

## HUMAN RIGHTS LEGAL FRAMEWORK

TfGBV and its discriminatory effects on women and LGBTI HRDs can have impacts on a range of human rights guaranteed under international human rights law (IHRL). This report is focused on the rights to freedom from gender-based violence, freedom of expression, freedom of peaceful assembly, freedom of association, privacy and an effective remedy, all protected by several treaties and declarations including the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), among others. Thailand has ratified these treaties and thus must comply with their obligations, including to respect, protect and fulfil these rights.

The Thai Constitution also guarantees various human rights, including the rights to non-discrimination, privacy, and freedom of expression and peaceful assembly. Despite the existing constitutional provisions, Thailand's domestic law lacks a robust framework for protecting women and LGBTI people from TfGBV in line with IHRL. While Thailand has adopted a law on combating gender-based discrimination, its application includes exemptions for discrimination committed in the name of religion or national security. In addition, the Thai government has proactively used existing cyber laws to prosecute online expressions by critics and provides no human rights-compliant legal safeguards for preventing the violation of the right to privacy.

Companies also have a responsibility to respect human rights wherever they operate in the world, as established by the UN Guiding Principles on Business and Human Rights (the UN Guiding Principles). A key part in fulfilling that responsibility is the adequate implementation of ongoing human rights due diligence, based on identifying, preventing, mitigating and accounting for the impact that the business has or may have on human rights. Where a company identifies through due diligence that it may cause or contribute to human rights abuse, it must cease or prevent its contribution to the adverse impact and provide remedy to those who have suffered the harm.

## TfGBV IN THAILAND

Amnesty International found that women and LGBTI HRDs in Thailand primarily endure two forms of TfGBV: targeted digital surveillance and online harassment. In many cases, some HRDs faced more than one form of TfGBV due to their activism.

TfGBV that results from targeted digital surveillance and online harassment may be due to intentionally discriminatory targeting, or because of the discriminatory effects experienced by survivors. Its impacts illustrated in this report are influenced by existing prejudices, biases and structural barriers experienced by the women and LGBTI HRDs due to their gender, sexual orientation, gender identity and/or expression and sex characteristics (SOGIESC) and human rights activism.

Amnesty International defines targeted digital surveillance as a practice of monitoring or spying on specific persons and/or organizations through digital technology to interfere with their private data. Amnesty International's research documents two cases of digital surveillance: the use of Pegasus spyware, and targeted attacks on individual Facebook accounts.

Pegasus, a spyware developed by NSO Group, allows unlimited access to a device without permission of the owner or operator and sends the information to another unauthorized entity, leaving little to no trace, so that the owner or operator of the device has almost no information as to what data was taken and who took it. Amnesty International classifies Pegasus spyware as a form of highly invasive spyware, on the basis that it can neither be independently audited nor limited in its functionality.

Among the 35 individuals in Thailand known to have been targeted with Pegasus spyware, 15 of them are men and 15 are cisgender women (the identities of the remaining five are unknown). Amnesty International was able to conduct interviews with nine of the 15 women targeted with Pegasus. These included those directly involved in the protest movement, and women HRDs campaigning and advocating for the rights of the protesters.

Technical and circumstantial evidence has led Amnesty International to conclude that 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. Such evidence includes the Thai government's past record of targeting HRDs who were under Pegasus attacks, existing technical investigations that indicated the use of Pegasus spyware in Thailand, and NSO Group's policy of selling its products exclusively to governments. This conclusion aligns with that of the National Human Rights Commission of Thailand (NHRCT), who announced on 5 April 2024 that "it cannot be denied" that a Thai government entity was responsible for the use of Pegasus against the targeted individuals in Thailand. Although the NHRCT said that the evidence pointed towards use of Pegasus by the Thai government, it was unable to identify which specific Thai government entity was responsible for the targeting. In response to these allegations, Thailand's Ministry of Foreign Affairs stated to Amnesty International: "[w]ith regard to the use of Pegasus spyware, there has not been any proven evidence as to which government agency has utilized the spyware".

In addition, Amnesty International spoke with six women and LGBTI HRDs who were among 44 activists in Thailand who reported having received a notification from Meta of "government-backed or sophisticated attacker alerts" via their personal Facebook accounts' support inbox on 17 November 2022. These HRDs are vocal critics of the government and/or the monarchy. Meta's Help Center indicates that this alert could include malicious attempts to "pose as someone you know or want to connect with – like a recruiter working in your industry – to trick you into befriending and communicating with them, sharing sensitive information, downloading malicious files, or clicking on malicious links designed to steal your passwords or other information" or to "passively [research] information about you to learn more about your online and offline activity".

This research assessed that this targeted digital surveillance had a gendered impact, resulting in fear and anxiety among HRDs that the private data about their lives could be weaponized against them through online harassment or used in court to prosecute them. Patcharadanai Rawangsub, a pro-democracy activist and HRD who identifies as a gay man, explained his concerns after learning that his Facebook account might be compromised:

**“[G]oing to prison is my worst nightmare. For gay men and trans women, Thai prisons can be brutal as you will most likely be sexually harassed and assaulted and face discrimination.”**

Protest leader Panusaya Sithijirawattanakul told Amnesty International that women HRDs are vulnerable to blackmail or attacks through the dissemination of their private data obtained through targeted surveillance. She said: "The effect of surveillance on women may not seem obvious to everyone at first, but women do have more to lose. Anything related to women's private lives could be picked up and used as a weapon against us to make us stop our activism."

Amnesty International also found that state and non-state actors have routinely weaponized online spaces to attack, intimidate and discredit women and LGBTI HRDs at least since the 2014 military coup. This research identified four common methods of online harassment against the HRDs: the use of hateful and abusive speech, targeted smear campaigns, doxing and threats of gendered violence.

The most common type of online harassment mentioned by almost every woman and LGBTI HRDs interviewed is the use of hateful and abusive speech. These attacks are laced with misogynistic, homophobic

and transphobic language. Many instances also involved sexualized content regarded as degrading or intimidating for women and LGBTI people.

Prominent HRDs, critics and activists reported to have experienced targeted smear campaigns through online platforms on which malicious actors post almost identical texts and images at roughly the same time in a coordinated manner to amplify the online attacks against their targets. The posts heavily featured the use of hateful and abusive language filled with gendered disinformation. The HRDs believed state and state-aligned actors to be behind these attacks.

Further, Amnesty International found that malicious unidentified actors have used doxing – the act of revealing personal or identifying documents or details about someone online without their consent – against many women, girls and LGBTI activists as a tactic of public shaming and intimidation. This research revealed that the personal data of many HRDs, including their home address, criminal record, roles in the protest movement and information related to their SOGIESC have been posted on social media platforms against their will.

Lastly, many women and LGBTI HRDs received threats of violence, including threats of force, killing and sexual assault, through social media platforms by means of public posts, comments and direct messages. In several cases, Amnesty International found that LGBTI HRDs who spoke out about LGBTI rights within the Muslim community faced this violent backlash online due to their activism.

In addition to the enduring and profound harm caused by TfGBV, women and LGBTI HRDs encountered multiple barriers to justice. The Thai government has denied its involvement in targeted digital surveillance and online harassment against women and LGBTI HRDs. Despite some efforts by the NHRCT, the government has failed to conduct thorough investigations to uncover all relevant information relating to these violations and ensure accountability for those responsible for them.

This research found that women and LGBTI HRDs struggled with gender insensitivity in the Thai criminal justice system. In several cases, police officers did not recognize the severity of TfGBV, leading to failures in registering and investigating complaints effectively.

Further, both judicial and non-judicial mechanisms proved inadequate in addressing TfGBV. The judicial system has also not delivered justice for those subjected to Pegasus spyware and targeted smear campaigns. Similarly, non-judicial mechanisms, designed to offer alternative avenues for seeking accountability, revealed significant limitations.

This research identified a growing chilling effect among women and LGBTI HRDs due to TfGBV. The mental health of the HRDs was severely affected after the compounding effect of experiencing violence in the digital space and finding themselves unable to seek accountability. As a result, they adapted their behaviours, developing distrust in the use of digital technology and limiting their expression or fully disengaging from activism.

In the Malay Muslim-majority SBPs, there is a noticeable pattern in which HRDs who work on LGBTI rights have chosen to refrain from using social media platforms altogether to avoid any potential TfGBV. “Of course, we do use digital tools, such as Line, to communicate with each other. However, within our group, we would not post anything about our activities on social media. It’s too dangerous,” said a Malay Muslim student activist who identifies as “gender-diverse”. He further added that he has seen many cases of Muslim people who openly shared on social media about their LGBTI identities, with such exposure leading to harassment by members of their own communities.

As prominent woman HRD Angkhana Neelapaijit, who has experienced targeted smear campaigns, explained:

**“Many women and LGBTI defenders are feeling isolated because there is little support when they experience gender-based violence online... Once we’re broken, there’s no way to repair ourselves. Often, many people are left with only one option: to walk away quietly and leave their activism behind”.**

# HUMAN RIGHTS IMPACTS OF TfGBV

“Thailand’s Ministry of Foreign Affairs informed Amnesty International to affirm that “Thailand has continued to demonstrate its commitment to advance the rights of women and girls, LGBTI, as well as human rights defenders” and add that “[t]hese groups have continuously been identified as our priority groups in the National Human Rights Plan. However, the various forms of TfGBV. However, the various forms of TfGBV documented by Amnesty International amount to violations of the rights to freedom from gender-based violence, freedom of expression, peaceful assembly and association, privacy and effective remedy of the targeted women and LGBTI HRDs.

The Thai state is directly responsible for these violations, as it is bound under IHRL to respect, protect and fulfil these rights. In many cases, it is difficult to unequivocally identify whether the Thai government took part in committing TfGBV, largely due to its lack of transparency and unwillingness to carry out effective investigations. However, at a minimum, in all the documented instances the government failed to protect the HRDs from the violations of the rights outlined above.

The Thai government has also failed to take sufficient action to ensure the right to an effective remedy for the HRDs subjected to TfGBV. This research indicates that the state failed to provide the women and LGBTI HRDs with access to relevant information concerning violations and reparation mechanisms; equal and effective access to justice; and adequate, effective and prompt reparation for harm suffered – the three components of this right required under IHRL.

NSO Group also failed to fulfil its responsibilities under the UN Guiding Principles, which provide that companies must respect all human rights. The company proceeded with the sale of Pegasus spyware, even though this highly invasive spyware does not include technical safeguards to ensure it does not cause human rights harm. Given these capabilities, any sale or use of this spyware cannot therefore be in line with IHRL.

Furthermore, if the NSO Group conducted human rights due diligence, it should have been aware of the history of digital repression against human rights activists and peaceful protesters in Thailand. With such knowledge, it would have had to be aware when it sold Pegasus spyware, including the sale that led to the violations described above (even if it did so through a distributor), that this product could or would cause direct human rights harm. At the time of publication, NSO Group had not replied to any of these allegations put to it by Amnesty International.

## CONCLUSION AND KEY RECOMMENDATIONS

Although Thailand continues to publicly position itself as a leader in gender equality, the testimony collected by Amnesty International indicates that this is far from the lived experience of women and LGBTI HRDs. The Thai government has failed to uphold the basic human rights of these HRDs guaranteed under international law. NSO Group has also failed to adequately respect its responsibility to respect human rights as set out in the UN Guiding Principles, given the role played by its Pegasus spyware in digitally surveilling women HRDs. To ensure compliance with IHRL, Amnesty International urges relevant actors to immediately adopt the following recommendations:

### TO THE GOVERNMENT OF THAILAND

Take immediate measures to address TfGBV against women and LGBTI HRDs by:

- Carrying out a prompt, independent, impartial and transparent investigation into all documented and reported instances of TfGBV against women and LGBTI HRDs, including but not limited to the use of unlawful targeted digital surveillance and online harassment mentioned in this research;
- Providing effective remedy in line with IHRL and standards to survivors of TfGBV, that are trauma-informed, survivor-centric and adopt an intersectional feminist approach, including by ensuring access to information about human rights abuses against them, guaranteeing equal and effective access to justice and providing appropriate reparations based on consultations with the survivors;
- Proactively removing structural and systemic barriers to gender equality, including by undertaking legislative measures, social policies and educational programmes to eliminate gender stereotypes,

negative social norms and discriminatory attitudes against women, girls and LGBTI people and create awareness about the phenomenon of TfGBV, its consequences and intersectional harms.

Adopt the following recommendations for ending unlawful targeted digital surveillance:

- 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.

Take the following actions to counteract the chilling effect and create a safe and enabling online and offline civic space, particularly for women and LGBTI people:

- End all criminal proceedings against all people, including women and LGBTI HRDs, charged solely for their involvement in peaceful protests or for exercising their right to freedom of expression
- Adopt a specialized protocol for law enforcement officials in addressing TfGBV through a gender-sensitive, trauma-informed response;
- Provide protection for women and LGBTI HRDs who wish to pursue legal actions for TfGBV to ensure they are safe from reprisals.

## **TO NSO GROUP**

- Cease the use, production, sale, transfer and support of Pegasus or other similar highly invasive spyware that can neither be independently audited nor limited in its functionality, given that technical safeguards and a human rights-respecting regulatory framework would still be insufficient to prevent their adverse human rights impacts;
- Provide adequate compensation and other forms of redress to victims of unlawful targeted surveillance through Pegasus spyware in Thailand.



**AMNESTY INTERNATIONAL  
IS A GLOBAL MOVEMENT  
FOR HUMAN RIGHTS.  
WHEN INJUSTICE HAPPENS  
TO ONE PERSON, IT  
MATTERS TO US ALL.**

#### CONTACT US



[info@amnesty.org](mailto:info@amnesty.org)



+44 (0)20 7413 5500

#### JOIN THE CONVERSATION



[www.facebook.com/AmnestyGlobal](https://www.facebook.com/AmnestyGlobal)



[@Amnesty](https://twitter.com/Amnesty)

# “BEING OURSELVES IS TOO DANGEROUS”

## DIGITAL VIOLENCE AND THE SILENCING OF WOMEN AND LGBTI HUMAN RIGHTS DEFENDERS IN THAILAND

As part of Amnesty International’s global flagship campaign Protect The Protest, this report tells the stories of women and LGBTI human rights defenders in Thailand who courageously sought to leverage digital technology for advancing their peaceful activism amid the shrinking civic space since the 2014 military coup. These defenders nonetheless faced technology-facilitated gender-based violence (TfGBV), including targeted digital surveillance and online harassment. The report further analyses the impacts of TfGBV in terms of producing a chilling effect among women and LGBTI defenders. Ultimately, TfGBV forces women and LGBTI people to limit or cease the exercise of their rights to freedom of expression and peaceful assembly, driving them out of the civic space and silencing their voices.