



**An ecosystem of
digital repression:
The silencing of women
human rights defenders
and other pro-democracy
activists in Myanmar**

An ecosystem of digital repression: The silencing of women human rights defenders and other pro-democracy activists in Myanmar

Author: Myanmar Internet Project (MIP)

Coordination and review: Verónica Ferrari and Pavitra Ramanujam (APC)

Editor: Alan Finlay

Proofreading: Zana Fauzi

Layout proofreading: Lynne Stuart

Design and layout: Japreet Saini

Publication production: Cathy Chen (APC) and Lori Nordstrom (APC)

Published by the Association for Progressive Communications (APC), 2026

Creative Commons Attribution 4.0 International (CC BY 4.0)

<https://creativecommons.org/licenses/by/4.0/>

ISBN 92-95049-52-7

APC-202604-APC-R-EN-DIGITAL-381

Table of contents

Executive summary	4
Introduction	5
An ecosystem of digital repression	8
Unpacking the different types of digital repression	10
State control over digital spaces: Myanmar’s repressive legislation	10
Internet shutdowns: Restricting freedom of expression and of information	12
Expanding surveillance mechanisms	13
Impact on WHRDs: Self-censorship, online violence and increased vulnerability	16
Criminalisation, surveillance and freedom of expression	16
Technology-facilitated gender-based violence (TFGBV) as tactic for digital repression	18
Increased vulnerability of women during internet shutdowns	19
Key findings	21
Recommendations	23
Key terms	25



Executive summary

00

Since the military coup in 2021, Myanmar has witnessed an alarming escalation in digital repression. The military junta has imposed internet shutdowns, deployed surveillance technologies and weaponised legal tools to silence dissent.

These tactics have disproportionately affected human rights defenders (HRDs), particularly women human rights defenders (WHRDs), who are subject to harassment and threats both online and offline and persecuted through the criminalisation of free speech.

This study, conducted by the Myanmar Internet Project (MIP) in collaboration with and support from the Association for Progressive Communications (APC), draws on a combination of desk research, case analysis and interviews. It documents and analyses the experiences of WHRDs and other pro-democracy activists to understand the lived realities of digital repression and gender-based violence under the military regime, while also integrating the insights of legal experts to clarify the legal context and implications of these violations.

Key findings

The research reveals that after the February 2021 coup in Myanmar¹ there have been various forms of digital repression, including surveillance, internet shutdowns and the amendment and enactment of laws affecting digital and internet rights. We refer to this as an “ecosystem” of digital repression, where all of these strategies are interdependent and work symbiotically to silence online dissent. This ecosystem has a differential impact on WHRDs in Myanmar. The research identified several forms of digital repression affecting them, including restrictions of free speech online, doxxing and sexual harassment through digital platforms such as Telegram. Internet shutdowns, meanwhile, have delayed vital support for women in need. The junta has also invaded the privacy of detained activists by downloading private photos off their phones and sharing them widely in an attempt to degrade and humiliate them. Moreover, we found that

¹ Freedom House. (2024). *Freedom on the Net 2024: Myanmar*. https://freedomhouse.org/country/myanmar/freedom-net/2024#foot-note3_jX2Amkm1tX7okLrg8AfZrv7AOPKXitMB5q2Lf6ca0_lGdvnU15OYv1

WHRDs who exposed cases of gender-based violence within the pro-democracy movement have been accused of attempting to undermine or discredit the revolution. Our findings show that the hostile digital environment has led to widespread self-censorship and what could be called the “digital disappearance” of women – those who choose to leave digital spaces due to the threats. Faced with constant surveillance, criminalisation and severe online harassment, many women defenders and activists are forced to withdraw from public and digital life to protect their safety and mental well-being. Many live in a constant state of uncertainty and fear, distrusting the digital technologies they rely on and that are necessary for their work.

The research provides critical evidence of the gendered nature of digital repression in Myanmar. The findings highlight the urgent need for protection and meaningful support for WHRDs and others who are on the frontlines of resistance.

Key recommendations

The report’s recommendations urge regional and international actors, including United Nations bodies, international organisations, the donor community, civil society organisations and tech companies to take coordinated action. This includes providing digital security training and tools to WHRDs, supporting safe and secure communication in the context of the surveillance state and funding psychosocial support for survivors of technology-facilitated gender-based violence (TFGBV). They also call for accountability measures against companies enabling surveillance and biometric data collection in Myanmar.

Introduction

01

Since the February 2021 coup in Myanmar,² there have been various forms of digital repression, including surveillance, internet shutdowns and the amendment and enactment of laws affecting digital and internet rights. Reports have highlighted targeted attacks against human rights defenders (HRDs), women human rights defenders (WHRDs) and other pro-democracy activists in the country, both offline and online. While the Freedom on the Net 2024 report by Freedom House stated that “activists, journalists, human rights defenders, and other dissidents have been regularly doxxed since the coup, usually over Telegram, TikTok, and Facebook,”³ Global Analysis 2022 by Front Line Defenders shows that WHRDs – in particular leaders in the post-coup Civil Disobedience Movement – have been “targeted with discriminatory tactics including public humiliation and verbal and sexual abuse by police and military forces.”

In response to the escalating repression, the Myanmar Internet Project (MIP) in collaboration with the Association for Progressive Communications (APC) undertook to document and analyse the various forms of digital repression used by the junta, and in particular to examine how these tactics have affected WHRDs and other frontline activists. The objective of the research is to inform international advocacy efforts, in particular digital rights policy advocacy led by civil society organisations and rights-based coalitions.

The study involved a qualitative analysis of reported instances of digital repression, including internet shutdowns, online attacks such as doxxing and accounts of online surveillance after the coup. Through desktop research, we also analysed the country’s legal framework, in particular the amendment and enactment of laws targeting the digital space. The literature review included United Nations (UN) documents, reports from local and international organisations such as Justice For Myanmar, Freedom House and Front Line Defenders, other civil society publications such as digital rights briefings, and relevant academic and media sources documenting digital repression in Myanmar.

Online interviews were also conducted with 10 WHRDs and other activists to gather first-hand insights on the incidents they have faced. Due to the country’s sensitive political situation,

2 Ibid.

3 Ibid.

interviewees have been anonymised to protect their identity.⁴ In order to gather different perspectives, WHRDs working in diverse fields, including but not limited to digital rights, and an individual identifying as LGBTQI+ were interviewed. While a number of interviewees have been forced into exile, two women activists residing inside the country were interviewed, of whom one had lived in an area affected by internet shutdowns. A human rights lawyer was also interviewed for legal analysis.

This report is organised in the following way. It begins by describing what this research refers to as the junta's ecosystem of digital repression, before elaborating on the different kinds of digital repression that we have identified. It then highlights key impacts of this digital repression on WHRDs and other activists. Following a summary of the study's findings, it offers detailed and action-orientated recommendations for stakeholders.

⁴ The numbered acronym KII for "key information interview" is used.

02

An ecosystem of digital repression

Since February 2021, the military junta has created what we call an “ecosystem” of digital repression to suppress online dissent, particularly targeting HRDs, WHRDs and other pro-democracy activists.

This ecosystem is sustained through three interconnected pillars:

- **The use of existing laws, subsequent amendments and new enactments to legitimise authoritarian actions:** Initiated shortly after the coup, the junta’s repressive strategy has steadily tightened its grip by amending laws and enacting new ones to legally justify its actions.
- **The implementation of internet shutdowns and censorship based on this legal framework:** Leveraging this legal framework, it has imposed numerous internet shutdowns, including blocking social media platforms, through the compliance of telecommunications and internet service providers.
- **The expansion of surveillance capabilities:** A crucial part of the repressive ecosystem is the widespread collection of the citizens’ personal data through multiple mechanisms including the forced collection of biometric information and mandatory mobile SIM card re-registration. Even before the coup, the Myanmar military had acquired surveillance tools and technology capable of retrieving historical data from devices, tracking signals and gathering social media intelligence from platforms. Since 2021, they have extended their surveillance capabilities to include web and network traffic monitoring, as well as profiling network behaviour.⁵ The junta also resorts to ground and financial surveillance to control activists and the public in general.

5 Al Jazeera. (2023, 15 January). Israel’s Cognyte won Myanmar spyware tender before coup. *Al Jazeera*. <https://www.aljazeera.com/news/2023/1/15/israels-cognyte-won-myanmar-spyware-tender-before-coup>

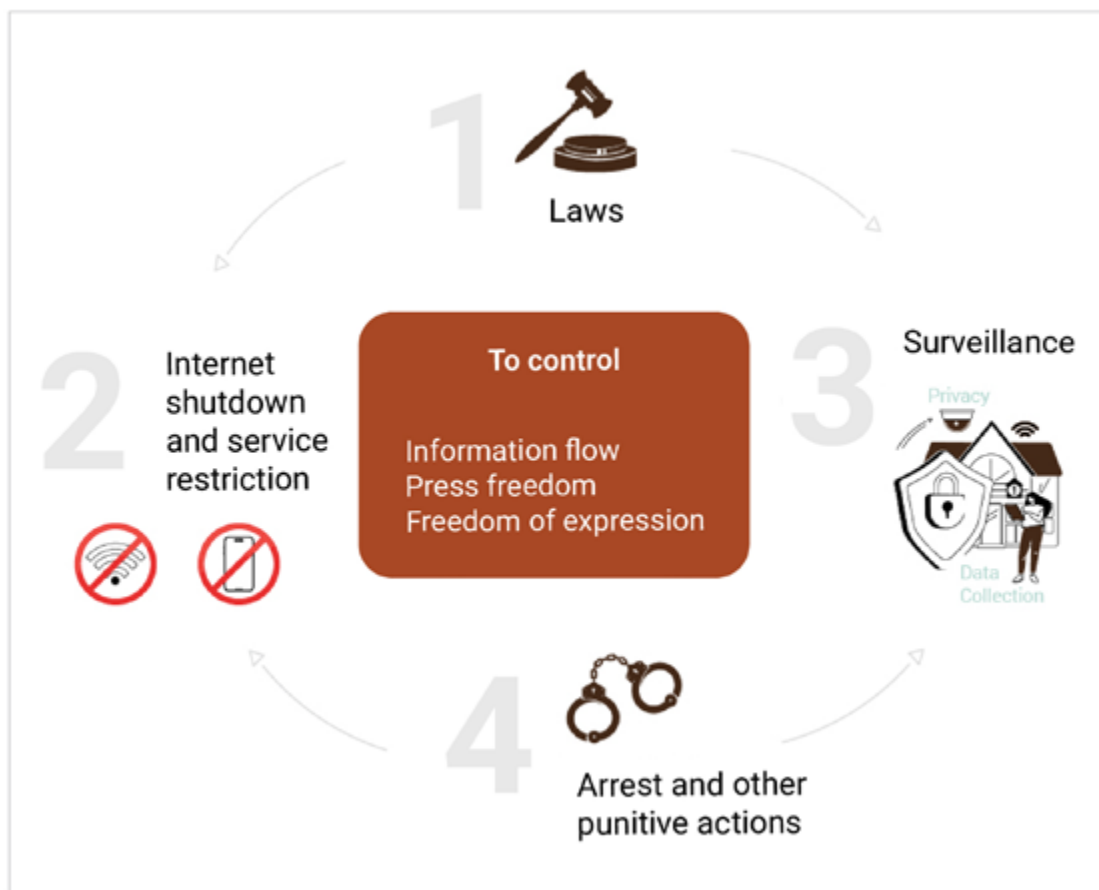


Figure 1 - Illustration of the junta's ecosystem of digital repression⁶

These mechanisms are intentionally designed to intimidate and control citizens, and to erode their privacy and fundamental rights by limiting access to information and suppressing freedom of expression. The overall impact is that through these comprehensive measures the junta has established significant control over citizens' privacy, freedom of movement, online expression and access to information, impacting their everyday activities. This has had far-reaching consequences for WHRDs and other pro-democracy activists residing within the country who are within reach of the junta's repressive apparatuses.

Unpacking the different types of digital repression

3.1

State control over digital spaces: Myanmar's repressive legislation

Since the February 2021 coup, the junta has unilaterally amended laws to suppress fundamental human rights including digital rights. This was done through the systematic dismantling of Myanmar's democratic institutions. The legislature was dissolved, executive power was concentrated in the hands of a military council called the State Administrative Council (SAC) and the judiciary has since functioned under the control of the junta, undermining judicial independence. These structural shifts have enabled the junta to enforce a repressive legal framework without checks and balances, facilitating widespread human rights abuses both offline and online.

In the aftermath of the coup, the junta weaponised legal reforms to legitimise surveillance and suppress online expression. It imposed seven major amendments and laws to monitor, criminalise and punish digital dissent. These were: amendments to the Law Protecting the Privacy and Security of Citizens;⁷ the revision of the Penal Code;⁸ the amendment of the Electronic Transactions Law;⁹ the amendment of the Broadcasting

7 <https://myanmar-law-library.org/law-library/laws-and-regulations/laws/myanmar-laws-1988-until-now/state-administration-council-2021/myanmar-laws-2021/state-administration-council-law-no-04-2021-amendment-of-law-protection-the.html>

8 https://www.law-democracy.org/wp-content/uploads/2025/10/Myanmar.Penal-Code-Analysis.Burmese.FINAL_.pdf

9 https://www.myanmar-responsiblebusiness.org/pdf/electronic-transactions-law_consolidated_2014-and-2021_my.pdf

Law;¹⁰ the promulgation of the Counter-Terrorism Law;¹¹ the amendment of the Union Taxation Law;¹² and the enactment of the Cybersecurity Law.¹³

Thirteen days after the coup, the junta revoked Articles 5, 7 and 8 of the Law Protecting the Privacy and Security of Citizens. Notably, Article 8(c), which barred interception of private communication, and 8(d), which prohibited authorities from demanding communication records without legal procedure, were revoked. This granted state actors unchecked access to citizens' data and eliminated safeguards against surveillance.

Similarly, on 14 February 2021, the junta arbitrarily amended sections 121, 124 and 500 of the Penal Code.¹⁴ Section 505, in particular, now criminalises actions that cause or intend to cause fear amongst citizens or the public as well as cause or intend to cause the spread of false news, knowing or believing that it is untrue.¹⁵ These vague provisions have been used to prosecute thousands.¹⁶

The research findings also indicate that the junta attempted to more effectively control internet users through amending the Electronic Transactions Law¹⁷ on 15 February 2021. It expanded the definition of "information" and included terms such as "video" and "application" in Section 2(a) of the law to broaden the scope of its jurisdiction. This has allowed the junta to criminalise users for sharing protest videos or using communications apps like Signal. Free Expression Myanmar reported that the amendment has seriously threatened freedom of expression and the protection of individual privacy,¹⁸ while Human Rights Watch stated that the amended Electronic Transactions Law prevents the free flow of information and criminalises the dissemination of information through cyberspace, including expression critical of the coup or the acts of the junta.¹⁹

Meanwhile, amendments to the Broadcasting Law in November 2021 removed previous exclusions of internet-based media, allowing the junta to prosecute online broadcasters. Punishment under this law was increased from fines to imprisonment, signalling a more aggressive clampdown on digital expression.²⁰

The new Counter-Terrorism Law promulgated on 1 March 2023 has also been used to strengthen the junta's surveillance net. Under Chapter 14, provisions were enacted

10 <https://myanmar-law-library.org/law-library/laws-and-regulations/laws/myanmar-laws-1988-until-now/state-administration-council-2021/myanmar-laws-2021/state-administration-council-law-no-63-2021-second-amendment-law-to-the.html>

11 https://sacoffice.gov.mm/my/bylaws_page

12 <https://myanmar-law-library.org/law-library/laws-and-regulations/laws/myanmar-laws-1988-until-now/state-administration-council-2021/myanmar-laws-2022/state-administration-council-law-no-01-2022-law-amending-the-union-tax-law-2021.html>

13 <https://mmlibrary.uwazi.io/en/entity/48w9o50foi6>

14 https://www.law-democracy.org/wp-content/uploads/2025/10/Myanmar.Penal-Code-Analysis.Burmese.FINAL_.pdf

15 https://myanmar-law-library.org/IMG/pdf/law_no_5-6_2021_sac_-2.pdf

16 <https://ispmyanmar.com/community/wp-content/uploads/2023/05/DM-44.pdf>

17 <https://www.myanmar-responsiblebusiness.org/pdf/electronic-transactions-law-consolidated-2014-and-2021-my.pdf>

18 Free Expression Myanmar. (2021, 18 February). Myanmar's new Electronic Transactions Law Amendment. <https://freexpressionmyanmar.org/myanmars-new-electronic-transactions-law-amendment/>

19 Human Rights Watch. (2021, 2 March). Myanmar: Post-Coup Legal Changes Erode Human Rights. <https://www.hrw.org/news/2021/03/02/myanmar-post-coup-legal-changes-erode-human-rights>

20 ARTICLE 19. (2021, December). Rebuilding an Architecture of Oppression: The impact of the military coup on freedom of expression and civic space in Myanmar. <https://www.article19.org/wp-content/uploads/2021/12/Rebuilding-an-Architecture-of-Oppression.pdf>

relating to the interception, restriction and shutdown of digital communications and electronic data, as well as the identification of user locations.²¹ These amendments are intended solely to justify interception, disruption, restriction and location tracking under the law. Through the inclusion of such provisions, the junta's surveillance of citizens communicating via telecommunications and online platforms may be perceived as legitimate under domestic law, despite being a clear violation of fundamental rights. As the human rights lawyer interviewed for this research observed:

They have framed it as legal and just, even though it is clearly a violation. [It is not] justice if someone has [the right] to intrude on another person's security, privacy or family life and watch them at any time. (KII-9)

Simultaneously, the Union Taxation Law was amended to raise SIM card prices from MMK1,500 (USD 0.71) to MMK20,000 (USD 9.52) and increased telecom taxes by 15%. These financial barriers serve to limit internet access and discourage online engagement.²²

Lastly, on 1 January 2025, the junta enacted the Cybersecurity Law, requiring internet service providers to retain user data for a minimum of three years.²³ This enables long-term profiling and the criminalisation of past speech or digital activity, and poses a risk for HRDs, WHRDs and other dissidents. An interviewee noted:

This clause enables authorities to arrest anyone at any time they choose. If someone does something the authorities oppose, they can look into the data and immediately accuse that person of a crime. These data were generated through interactions between service providers and users. It infringes on the property rights that are integral to digital rights. (KII-9)

3.2

Internet shutdowns: Restricting freedom of expression and of information

Following the coup, the SAC has used internet shutdowns to suppress free speech and restrict the flow of information, impacting both the general public and human rights activists.

Since the beginning of 2021, there have been at least six nationwide internet blackouts²⁴ and over 420 shutdowns targeting specific regions where local crises intensified.²⁵ According to a joint statement released by digital rights organisations in Myanmar on 31 March 2025, more than 100 townships have experienced internet shutdowns,²⁶ many

21 https://www.myanmarinternet.info/my/post/blog_006

22 Myanmar Internet Project. (2024, 10 November). Myanmar Digital Coup Quarterly: August 2024 to October 2024. <https://www.myanmarinternet.info/my/post/quarterly-report-004>

23 https://www.myanmarinternet.info/my/post/cyber_law_in_myanmar

24 <https://www.myanmarinternet.info/internet-shutdown>

25 Ibid.

26 Myanmar Internet Project. (2025, 1 April). Joint statement: Myanmar must lift internet restrictions following devastating earthquake. <https://www.myanmarinternet.info/post/joint-statement-myanmar-must-lift-internet-restrictions-following-devastating-earthquake>

in conflict-affected areas or those controlled by the resistance. Notably, on 15 February 2021 nightly internet blackouts – referred to as “internet curfews” – were imposed from midnight to 9 a.m.,²⁷ restricting communication during critical hours of coordination.

The junta has also targeted social media platforms. Widely used platforms including Facebook, Twitter and Instagram were first blocked right after the coup, on 4 and 5 February 2021.²⁸

In response, activists have turned to virtual private networks (VPNs) to bypass restrictions and access the platforms. However, on 30 May 2024, the SAC attempted to restrict the use of VPNs by employing advanced technologies.²⁹ This included advanced firewall systems and network intelligence tools, with capabilities such as deep packet inspection (DPI) to analyse user data.³⁰ According to a Justice For Myanmar report, the project to block VPNs was awarded to Mascots Technologies, with technical support from Chinese companies Geedge Networks and the China National Electronics Import and Export Corporation (CEIEC).³¹

3.3

Expanding surveillance mechanisms

Several forms of surveillance are critical to the ecosystem of digital repression that has been established in Myanmar.

Data collection and biometric surveillance

The junta first strengthened its surveillance capabilities by enforcing mandatory SIM card re-registrations in order to track people’s communications.³² In 2023, the Ministry of Immigration and Population, under the junta’s directive, also pushed to collect the biometric and biographic data of citizens.³³ This has included fingerprint and iris scans and recording detailed personal information such as current address, occupation and family status. It was also announced that the data from the SIM Registration Management System, shared by the Posts and Telecommunications Department, would be cross-checked against the database of the Ministry of Immigration and Population.³⁴ By combining data collected from SIM registration with biometric and biographic data, the junta is able to easily monitor the public’s movements within the country, and have the biographical details of any person they are monitoring ready at hand.

27 Al Jazeera. (2021, 16 February). Myanmar blocks internet for second night in bid to choke protests. *Al Jazeera*. <https://www.aljazeera.com/news/2021/2/16/myanmar-blocks-internet-for-second-night-in-bid-to-choke-protests>

28 Reuters. (2021, 7 April). Myanmar’s internet suppression. Reuters. <https://www.reuters.com/graphics/MYANMAR-POLITICS/INTERNET-RESTRICTION/rlgpdbreepo/>

29 Access Now. (2024, 26 June). Worse than China or Iran? Myanmar’s dangerous VPN ban. <https://www.accessnow.org/myanmar-vpn-ban/>

30 <https://www.facebook.com/100067770862498/posts/78158447077241/?mibextid=oFDknk&rdid=h2JbHnlaw2jTEBP>

31 Justice For Myanmar. (2024, 19 June). The Myanmar junta’s partners in digital surveillance and censorship. <https://www.justiceformyanmar.org/stories/the-myanmar-juntas-partners-in-digital-surveillance-and-censorship>

32 <https://www.moi.gov.mm/index.php/news/34298>

33 <https://dop.gov.mm/en/news/2454>

34 Ibid.

AI-enhanced ground surveillance

While implementing the large-scale data collection process is important for mass surveillance, the junta has also deployed ground surveillance technology. In 2022, closed-circuit television (CCTV) networks equipped with AI facial recognition capabilities were deployed in cities including Mawlamyine, Dawei, Taunggyi, Hpa-An and Myitkyina.³⁵

One activist interviewed described how her group was targeted:

After an activity, the junta forces tracked their vehicle number through CCTV footage. It was at the time of the crackdown. They tracked the vehicle using its licence plate to find out who owned it and who had rented it. From there, they made connections. If the car was rented, there would surely be a phone number. That's how they got the phone number. Finally, they intercepted phone calls and monitored exactly who was talking to whom and how the meetings were arranged. Members of our group experienced arrests as a result of that surveillance. (KII-8)

Financial surveillance through mobile money

It was found that the junta also surveilled financial transactions. Its financial surveillance system extended to monitoring mobile money transactions, evident from the freezing of user accounts on mobile money services.³⁶ Financial transactions on mobile money platforms, which require account registration primarily through mobile phone numbers, are vulnerable to surveillance as they can be easily linked to the personal data of citizens collected by the junta. A WHRD working on gender-based violence described how financial surveillance is being used to target activists: "One of the members of my organisation, her personal KPay³⁷ account accepts the funding for the activities. They tracked her through her KPay account and came to arrest her at home." (KII-4)

Online monitoring by pro-junta groups, and doxxing as digital warfare

While the junta has implemented a surveillance system using advanced technology, pro-junta groups monitor online social media activity identifying individuals for attack. This is a form of non-state surveillance that should be considered part of the overall surveillance mechanism supporting the coup. Forms of attack have include sharing the private information of individuals, such as addresses and phone numbers – or doxxing – on pro-junta channels,³⁸ which Myanmar Witness describes as the digital manifestation of the real-world violence faced by thousands of people in Myanmar every day. Social media users have been detained as a result of incitement on Telegram channels run by pro-junta groups.³⁹

35 Potkin, F. (2022, 10 July). Myanmar's junta rolls out Chinese camera surveillance systems in more cities. *Reuters*. <https://www.reuters.com/world/asia-pacific/exclusive-myanmars-junta-rolls-out-chinese-camera-surveillance-systems-more-2022-07-10/>

36 <https://burma.irrawaddy.com/news/2022/09/21/254726.html>

37 KPay is a short form of KBZ Pay, a mobile wallet, powered by KBZ bank, Myanmar's privately owned bank.

38 Anlezark, D. (2023, 17 October). Myanmar's growing doxxing problem. *Index on Censorship*. <https://www.indexoncensorship.org/2023/10/myanmars-growing-doxxing-problem/>

39 https://www.myanmarinternet.info/my/post/surveillance_ecosystem_over_four_years

One of the women activists interviewed during this research explained how the pro-junta groups work:

If you figure out the posts from channels such as Han Nyein Oo,⁴⁰ we can clearly see that once they get some information from one platform, they cross-check it with another. Suppose someone commented on anti-junta media pages like Khit Thit. They check first this account is public. If it is, they find the account holder's personal information such as business, job or school. After that they dox through their channels. (KII-3)

Another interviewee suggested how doxxing intensifies already threatening experiences: "She experienced [things] such as the arrest of her family members and the blocking off of her house. She also experienced doxxing on Telegram." (KII-5)

The co-option of the private sector

A recent report by Justice For Myanmar has accused 13 telecoms providers operating in the country of complicity in state surveillance.⁴¹ While telecommunications companies are complicit either voluntarily or through being forced by the junta to co-operate, not all private sector companies have complied. Justice For Myanmar reported in March 2022 that interception and surveillance systems had been installed on the network of the telecommunications company Telenor.⁴² Telenor responded by deciding to stop operations and exit the country, admitting that it was due to pressure to install the systems.⁴³

40 Han Nyein Oo is a prominent pro-military propagandist who has consistently amplified junta-aligned narratives and disinformation on social media before and after the 2021 coup, often targeting pro-democracy actors and independent media.

41 Justice For Myanmar. (2025, 9 September). Silk Road of Surveillance. <https://www.justiceformyanmar.org/stories/silk-road-of-surveillance>

42 Justice For Myanmar. (2022, 5 March). Telenor Group violating sanctions through installation and imminent transfer of German Lawful Intercept Gateway. <https://www.justiceformyanmar.org/press-releases/telenor-group-violating-sanctions-through-installation-and-imminent-transfer-of-german-lawful-intercept-gateway/>

43 <https://burma.irrawaddy.com/news/short-news/2021/09/15/246021.html>

Impact on WHRDs: Self-censorship, online violence and increased vulnerability

4.1

Criminalisation, surveillance and freedom of expression

The junta's post-coup legal framework has resulted in the systematic repression of digital rights and freedom of expression in Myanmar, with the threat of being criminally prosecuted creating a climate of uncertainty and fear for WHRDs. Between 2021 and 2023, over 2,000 people were imprisoned under Section 505(a) of the Penal Code, including artists,⁴⁴ former ministers,⁴⁵ journalists and ordinary citizens that expressed dissent against the regime.⁴⁶ Data for Myanmar reported that 1,691 individuals were arrested due to their online speech from February 2022 to July 2024.⁴⁷ According to the SAC website,⁴⁸ out of 374 individuals detained due to online speech in 2024, 114 of them were women.

WHRDs now operate in an environment where their work, speech or even private communication can be considered criminal behaviour under the sweeping laws. Prominent examples of the persecution of women include: the arrest on 29 April 2022 under the Counter-Terrorism Law of Daw Ywat Nu Aung, a lawyer who had been representing leaders of the National League for Democracy (NLD), and who was

44 <https://www.facebook.com/100018589237370/posts/pfbid031BwzWxLJHb9yVERo3LWghUsKwDUy9MSxtXXKn6Le8aU-wTcjysfAwZ6L1MbbXLTCEI/>

45 <https://news-eleven.com/article/284766>

46 Strangio, S. (2023, 4 May). Myanmar junta pardons more than 2,000 political prisoners. *The Diplomat*. <https://thediplomat.com/2023/05/myanmar-junta-pardons-more-than-2000-political-prisoners/>

47 <https://tinyurl.com/mrhwp9ax>

48 <https://myanmar.gov.mm>

sentenced to 15 years of hard labour;⁴⁹ the arrests of labour rights activist Daw Myo Myo Aye⁵⁰ and Burmese freelance journalist and former BBC Media Action presenter Htet Htet Khine,⁵¹ both prosecuted under Penal Code 505; and the prosecution of filmmaker Ma Eaint⁵² who is currently serving a three-year sentence under the same section of the Penal Code for an alleged donation to the resistance forces. The news website Irrawaddy revealed that her toes were fractured during a brutal interrogation process.⁵³

The legislative tools work hand in hand with the surveillance network that has been established by the junta which is used to monitor and control the public in general, and activists in particular. Interviewees said that the surveillance measures have forced WHRDs to change their digital security habits. While activists have had to upskill to use new, safer digital tools, better security also has a financial cost. Changes have included replacing SIM cards, switching digital devices, locking social media profiles, using pseudonyms on social media and using Signal for secure communication. However, activists are still left with a pervasive sense of uncertainty and vulnerability. As one WHRD we interviewed stated: "This unknown situation about how much surveillance is through the digital devices, and how dangerous the digital devices are to us, has made us fearful." (KII-5)

This fear has led many WHRDs to self-censor what they say as they "[worry that] their actions can be criminalised." (KII-2). A 2023 research report by the Gender Equality Network (GEN) and MIP called *Technology: Friend or Foe for Women of Myanmar* stated that 92.5% of women participants who were included in the study believed that the freedom of expression of women has declined.⁵⁴

Another WHRD interviewed for this research suggested that this decline in freedom of expression was noticeable in fewer people being outspoken on rights issues in the media:

They arbitrarily amend and enact laws as they wish. Because these amendments and enactments are intended for repression, individuals engaged in rights-based activities have disappeared from the media. (KII-6)

Many have been forced into exile as a result of the repressive measures, as in the case of one of the activists interviewed for this research: "After a warrant under Section 505 was issued against me, I eventually faced a situation where I had to flee to the border." (KII-1)

49 <https://myanmar-now.org/mm/news/11143/>

50 <https://www.dvb.no/post/458130>

51 CIVICUS Monitor. (2022, 31 December). Journalists and activists continue to be given long jail sentences on fabricated charges nearly two years on from the illegal coup. <https://monitor.civicus.org/explore/journalists-and-activists-continue-be-given-long-jail-sentences-fabricated-charges-nearly-two-years-illegal-coup/>

52 <https://burma.irrawaddy.com/news/2022/04/30/251616.html>

53 <https://burma.irrawaddy.com/news/2021/06/29/243587.html>

54 Gender Equality Network and Myanmar Internet Project. (2023). *Technology: Friend or Foe for Women of Myanmar*. <https://mmlibrary.uwazi.io/en/entity/spm6ywwlnp>

Technology-facilitated gender-based violence (TFGBV) as tactic for digital repression

Women have historically played a pivotal and highly visible role in Myanmar's political and civic life, from grassroots activism to leadership in pro-democracy movements. Since the 2021 coup, however, women's rights have faced a severe backslide amid an environment of escalating violence. Between February 2021 and December 2024, the Women's League of Burma documented the killings of 1,344 women and the arrest of 5,027 as a result of the junta's violence.⁵⁵ The UN Secretary-General, in his 2023 report to the Security Council, noted that sexual violence, including the threat and use of rape, has been used in Myanmar "as part of the repertoire of political violence to intimidate and punish opponents, their family members, and women human rights defenders."⁵⁶

This backsliding of women's rights is also evident in resistance-controlled areas. Several WHRDs reported retaliatory attacks from members of the revolutionary forces for exposing cases of domestic violence, with accusations of "undermining the revolution" used to silence them (KII-4). Similar threats targeted women's rights organisers who challenged male-only public panels, forcing them to undertake security risks assessments for their events (KII-10).

Within this wider context of violence, women's participation in Myanmar's digital sphere has faced a significant challenge due to targeted online abuse and digital repression. According to research jointly released by Sisters to Sisters and Myanmar Witness, "online abuse of Myanmar women who are actively involved in politics was at least five times more prevalent at the end of 2022 compared with the weeks following the coup."⁵⁷ The research also highlighted that the "overall prevalence of abusive posts targeting women on Telegram was up to 500 times higher than international baselines for abuse prevalence on social media, where these exist."

Moreover, it stated that "90% of abusive posts in its qualitative analysis were authored or shared by pro-SAC accounts." It said that "many targeted women were not well-known, and appear singled out simply for positively commenting on pro-People Defence Forces (PDF) or National Union Government (NUG) posts."

Freedom House's Freedom on the Net report 2024 also found that women activists who opposed the coup suffered sexual harassment.⁵⁸ The report highlighted specific online tactics, such as doxxing on platforms like Telegram, Facebook and TikTok. Echoing the report by Sisters to Sisters and Myanmar Witness, Freedom House noted that this abuse did not only target politically active women: "Women and girls self-censored on a range of

55 <https://www.womenofburma.org/sites/default/files/2025-05/Databased%20for%20Violence%20Against%20Women%20by%20Year.pdf>

56 Andrews, T. (2024). *Courage amid crisis: gendered impacts of the coup and the pursuit of gender equality in Myanmar*. <https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session56/a-hrc-56-crp-8.pdf>

57 Myanmar Witness. (2023, 27 January). Digital Battlegrounds: Politically motivated abuse of Myanmar women online. *Centre for Information Resilience*. <https://www.info-res.org/cir/reports/digital-battlegrounds-politically-motivated-abuse-of-myanmar-women-online/>

58 Freedom House. (2024). *Freedom on the Net 2024: The Struggle for Trust Online*. <https://www.freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf>

topics, particularly those related to sex and gender, due to the risk of abuse and sexual harassment”.

The LGBTQI+ activist we interviewed recounted:

We called for action on social media and rallied under “Our sarong, our flag, and our victory” as a solidarity movement for women under systemic repression. Under [our post], we saw a lot of comments [amounting to] sexual harassment. Some of us experience a lot of sexual harassment with people sending inappropriate images in our chat boxes. (KII-1)

The 2023 study by GEN and MIP also found that the private photos of WHRDs – obtained by accessing the mobile phones of arrested women – were distributed through Telegram accounts affiliated with the SAC.

A woman political activist we interviewed shared her experience:

I had a severe allergic reaction and took photos of my whole body at that time. Since my entire body was affected, I took some photos with less clothing to keep for documentation. They took these photos and kept them separately in their phones. They distributed them widely. While I was in detention, they would come and verbally harass me, saying things like “I’ve already seen your photos. Wow, you look really hot.” That kind of harassment happened to me. (KII-8)

4.3

Increased vulnerability of women during internet shutdowns

Internet shutdowns, including the blocking of platforms to prevent the public from using the internet for everyday communications, disconnect people from each other and stop the flow of crucial information in times of crisis. This research showed that there were instances where they placed WHRDs at increased physical risk and prevented vulnerable women from finding the vital support services they needed.

A WHRD described the impact of these shutdowns on the safety of the journalists she works with who are exposed to unnecessary physical risks as they try to get online:

For female journalists, they can’t pay attention to their own security due to internet difficulties. They have to go up hills or to remote places just to get access and that increases risks of violence.

She described how being unable to communicate also created a climate of concern and alarm:

One of the journalists from Rakhine State committed to join our training. Then she disappeared for two months. There was no internet, no mobile phone connection – we didn’t even know what had happened to her. Situations like that do happen. (KII-7)

Shutdowns have also obstructed services set up to support female victims of violence. A WHRD working on gender-based violence reported:

Some victims have to travel to places where Starlink connections are available due to the internet shutdowns. Just to meet with us or talk, they have to find a spot where they can get some voice out. Sometimes, in urgent situations, we can't even connect to them. (KII-4)

One of the WHRDs interviewed suggested that although VPNs could be used to bypass the blocking of social media sites, they complicated their outreach activities and were not necessarily useful for women who lacked digital skills:

The situations that depend on VPNs and the blocking of mainstream social media platforms negatively affected the outreach of our activities. Individuals who are not familiar with technology were delayed in contacting us, as they could not easily connect via social media platforms. Mainly, in the support programme, there was a delay. (KII-4)

Key findings

05

The digital repression in Myanmar has created deeply hostile conditions, particularly for WHRDs and other pro-democracy activists. These conditions are the result of the coordinated use of legislation, surveillance, and internet shutdowns or what we refer to as an “ecosystem” of digital repression. The impact is multifaceted: a climate of fear and uncertainty, pervaded by physical, psychological, legal and digital insecurity, that has forced many activists to censor themselves, and others into exile.

The following are the key methods of digital repression used by the junta:

- **Repressive legal frameworks:** The junta’s amended and newly enacted laws have enabled the arbitrary prosecution of WHRDs and other pro-democracy activists, criminalising peaceful expression, digital organising and dissent.
- **Internet shutdowns:** Internet shutdowns have interrupted the flow of information, free speech, and restricted support services for those in need. Activists have had to rely on VPNs to try to bypass these restrictions, but this has negatively affected outreach activities.
- **Expansion of surveillance:** The surveillance apparatus has been expanded through the collection of biometric data and the forced re-registration of SIM cards. The ability to track WHRDs is bolstered through the use of a CCTV network equipped with AI facial recognition technology. Mobile money accounts are also monitored, while activists have to contend with the organised non-state monitoring of social media and doxxing by pro-junta groups.

The following are the key gendered impacts these methods have on the work of WHRDs:

- **The threat of arrest, self-censorship and uncertainty:** The criminalisation of dissent has created a climate of fear and uncertainty for WHRDs in the wake of arrests and reports of assault while in custody. Activists self-censor to protect themselves. The threat of prosecution combined with the ubiquitous surveillance system has led some to distrust the digital tools essential to their work and survival.

- **TFGBV:** WHRDs face widespread sexual harassment and threats online. These attacks have led to lasting psychological trauma and, in some cases, physical harm. These attacks have come from pro-junta groups, but the junta has also invaded the privacy of detained activists by downloading private photos off their phones and sharing them widely in an attempt to degrade and humiliate them. Meanwhile WHRDs have faced backlash, threats and retaliation from within resistance movements when reporting or speaking out about abuse.
- **Increased vulnerability of women during internet shutdowns:** Internet shutdowns have placed WHRDs and women in general at greater risk. WHRDs are forced to travel to remote or unsecure areas to get online, exposing them to increased risks or violence. Shutdowns have also obstructed services set up to support victims of gender-based violence, and other forms of support for women.

Recommendations

Based on research findings, the following recommendations are made to address Myanmar's escalating digital repression and its gendered impacts on WHRDs and other activists.

6.1

International community (multilateral actors and states)

i. **Hold the military accountable for the use of repressive laws as tools of persecution:**

Since the 2021 coup, the junta has unilaterally enacted or amended laws to criminalise dissent, detain WHRDs and legitimise repression. These laws are not the result of a legislative process and fundamentally violate international human rights standards, including the International Covenant on Civil and Political Rights (ICCPR) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), among other instruments.

We urge UN bodies and international actors to:

- Publicly denounce these laws as tools of political persecution.
- Support investigations into how the use of these laws result in human rights abuses.
- Advance accountability through international accountability mechanisms.
- Call for an end to all internet shutdowns in Myanmar. Ensure accountability for actors involved in enabling shutdowns and fund alternative connectivity tools in affected areas.

ii. **Take action against companies that enable surveillance:** Investigate and sanction companies supplying surveillance technologies, including biometric systems and data interception tools that are enabling the junta's digital repression. These companies are complicit in human rights violations. In line with international human

rights instruments, such as the Freedom Online Coalition's Guiding Principles on Government use of Surveillance Technologies, it is required that companies:

- Conduct human rights due diligence assessments before concluding sales or entering into partnerships.
- Refuse contracts where surveillance lacks legality, necessity or proportionality.
- Publish transparency reports on demands made by the junta to interrupt or block services, as well as on its deployment of technology.
- Cease sales and withdraw support where there is evidence of abuse.

6.2

Digital platforms and tech companies

- i. **Remove harmful content and improve platform accountability:** Platforms like Telegram, Meta and TikTok are being used to target WHRDs through hate speech, sexual harassment and doxxing, especially in the local languages, mainly in Burmese.

We call on these companies to:

- Improve content moderation systems and invest in local language and context capacity expertise.
- Ensure user data protection, reject illegitimate demands by the junta to interrupt or block services and publish detailed transparency reports.
- Conduct regular human rights due diligence assessments across operations, with special attention to contexts of conflict and repression.

- ii. **Collaborate with human rights civil society organisations:** Given that WHRDs are deliberately targeted on platforms by pro-junta groups we urge the platforms to coordinate with human rights and digital rights organisations to:

- Establish trusted partner channels with civil society and develop rapid-response protocols for victims of TFGBV and coordinated online attacks.
- Establish secure channels to escalate threats when users need urgent protection, such as when they are at risk of being arrested due to being targeted online by pro-junta groups.
- Share non-personal, aggregated data on threats when coordinated harassment and disinformation campaigns are evident.
- Develop joint protocols for verifying and acting on content that endangers WHRDs and other pro-democracy activists, ensuring rapid takedown where necessary.
- Involve local organisations in product and service safety reviews and policy changes affecting at-risk communities.

- iii. **Tech companies should not enable repression and must uphold human rights standards:** Beyond social media platforms, other tech companies play a critical role in enabling and resisting digital repression.

We call on:

- Telecom and internet service providers to not comply with surveillance demands made by the junta and ensure the continuity of secure and reliable communication services.
- Connectivity providers, including satellite companies, to prioritise access for humanitarian and civil society purposes, and to safeguard these services from restrictions imposed under junta pressure.
- Companies supplying surveillance, interception or biometric technologies to Myanmar to immediately suspend sales that enable repression, and for international regulators to apply strict human rights due diligence and export controls in line with the UN Guiding Principles on Business and Human Rights and related international standards.

6.3

International non-government organisations (INGOs) and donor organisations

INGOs and donors have a crucial role to play in supporting WHRDs and other pro-democracy activists and raising awareness of digital repression in Myanmar.

We urge INGOs and donors to:

- i. **Provide digital security support:** As Myanmar has become a surveillance state, it is increasingly difficult and dangerous for WHRDs and other activists to communicate securely. Beyond the financial burden of replacing devices and SIM cards, defenders face rising risks of interception, tracking and digital profiling. INGOs and donors should invest in robust digital security support, including tailored training, and the development of secure tools and trusted connectivity alternatives for those operating in high-risk or shutdown areas.
- ii. **Support rehabilitation programmes:** Due to doxxing, online sexual harassment and other threats, WHRDs in particular suffer serious psychological and even physical harm. Donors should prioritise mental health services to support traumatised activists, including creating safe houses and rehabilitation programmes as part of broader protection strategies.
- iii. **Mobilise international solidarity and advocacy:** Increased coordination among regional and global civil society actors to amplify the crisis of digital repression in Myanmar is necessary. This includes raising the profile of research into the conditions of digital repression in Myanmar in international advocacy spaces, producing joint statements and influencing relevant UN and multilateral mechanisms.

Digital rights, human rights and women rights activists and organisations in Myanmar

Civil society organisations in Myanmar need to ensure that they do not inadvertently contribute to the repression of WHRDs through their activism.

We strongly urge civil society organisations to:

- i. **Promote gender justice within the resistance movements:** Gender-based violence is not limited to state repression, it also occurs within pro-revolutionary groups. WHRDs who raised concerns are often branded as undermining the revolution. We urge all contributors to the democratic movement, both internal and external, to uphold feminist principles, prioritise gender justice and commit to inclusive accountability.

Key actions for resistance movement leadership and stakeholders:

- **Develop policies on TFGBV:** Establish clear, community-defined codes of conduct that explicitly condemn all forms of gender-based violence, including TFGBV. Facilitate safe, confidential pathways for WHRDs to raise concerns without fear of retaliation. Create policies that are applicable to both offline and online harassment.
- **Ensure meaningful inclusion:** Elevate WHRDs into leadership roles and decision-making spaces and include them in strategy sessions. Ensure their voices shape policy and action.
- **Practice transparent accountability:** When abuses emerge, whether offline or online, commit to impartial investigations, restorative remedies and actions that reinforce a culture of justice. This institutional clarity reinforces feminist values and builds trust.

Key terms

07

Doxxing: A form of targeted online attack where the private information of individuals, such as addresses, phone numbers and communications, is exposed without their consent, often occurring on platforms like Telegram, TikTok and Facebook.

Ecosystem of digital repression: Refers to the junta's symbiotic use of technology and legal tools to monitor, control and silence dissent. This includes enforcing repressive laws, deploying mass surveillance and implementing internet shutdowns, tactics amplified by online attacks like doxxing and harassment by pro-junta groups. These strategies in particular target WRHDs and other pro-democracy activists.

Financial surveillance: Monitoring financial transactions, including those conducted on mobile money platforms, which can be linked to citizens' personal data.

Gender: Gender refers to the characteristics of women, men, girls and boys that are socially constructed. This includes norms, behaviours and roles associated with being a woman, man, girl or boy, as well as relationships with each other. As a social construct, gender varies from society to society and can change over time.⁵⁹

Human rights defenders (HRDs): All persons, who individually or in association with others, act to promote or protect human rights peacefully.⁶⁰ In the context of digital rights, they advocate for human rights online as well as for equal access to new technologies and work to bridge digital divides.

Internet curfew: In the context of Myanmar, refers to nightly internet blackouts imposed from 1 a.m. to 9 a.m.

59 https://www.who.int/health-topics/gender#tab=tab_1

60 <https://www.ohchr.org/en/special-procedures/sr-human-rights-defenders/about-human-rights-defenders>

Internet shutdowns/internet blackouts: Measures taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online.⁶¹ This report makes specific reference to internet blackouts, or the complete or partial failure of the internet services, and the blocking of social media platforms by the junta, which means users cannot access these specific platforms.

Repressive legislation: Seven major amendments and laws enforced by the junta after the coup to expand state control over digital spaces, legitimise surveillance and silence critical voices.

Technology-facilitated gender-based violence (TFGBV): Encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms and email. Includes cyberstalking, online harassment and doxxing.⁶²

Women human rights defenders (WHRDs): Refers to women who work peacefully, individually or in association with others, to promote and protect human rights. The term also includes people of any gender who work on issues related to women's rights and gender equality.

61 Office of the United Nations High Commissioner for Human Rights. (2022). *Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights*. A/HRC/50/55. <https://www.ohchr.org/en/documents/thematic-reports/ahrc5055-internet-shutdowns-trends-causes-legal-implications-and-impacts>

62 <https://www.unfpa.org/TFGBV>

