HUMAN RIGHTS MYANMAR

# Impact of AI and the digital dictatorship on cultural life in Myanmar

Submission to the UN Expert Mechanism on the Right to Development – December 2025

## Introduction

Since the 2021 coup, the military has systematically weaponised digital technology and Artificial Intelligence (AI) as core components of its strategy to silence dissent and consolidate power. This digital coup has resulted in a significant collapse of civil and political rights, fundamentally altering the landscape for the right to development and cultural rights in Myanmar. The digital sphere is no longer a neutral space for development but a domain where fundamental rights are being systematically dismantled and denied.

This submission to the UN Expert Mechanism on the Right to Development demonstrates that in the current context, AI does not serve as a tool for cultural or economic advancement. Instead, it has been integrated into a digital dictatorship designed to automate censorship, enforce a climate of fear, and erase those who oppose the military regime.

## Legal architecture enabling AI repression

The deployment of automated surveillance technologies in Myanmar relies on a repressive legal framework designed to strip people of data privacy and legitimise state violence. Rather than regulating technology to protect human rights, these laws deregulate the State's use of surveillance while criminalising the civil society actors who might otherwise check these systems.

- **Organisation Registration Law (2022):** By preventing the establishment of NGOs and criminalising unregistered NGOs, this law effectively bans independent rights groups. It eliminates the only mechanism capable of monitoring AI harms or demanding transparency, ensuring surveillance technologies are deployed without civil society oversight.
- **Counter-Terrorism Law (2014):** Legitimises automated monitoring, tracking transactions to flag donors supporting the pro-democracy movement. Mobile money platforms like KBZPay and Wave Money reportedly hunt down donors. Article 52(a) converts these digital footprints into criminal evidence, arresting artists and activists for supporting or financing "terror" simply for conducting cultural resistance online.

- **Constitution (2008):** Broad security exceptions in Article 354 provide constitutional cover for mass surveillance. The regime argues that imported facial recognition cameras and automated monitoring are necessary for "community peace", effectively overriding the right to privacy essential for cultural self-determination.
- **Penal Code (1861):** Defines illegal content for automated monitoring tools. Broad provisions against "causing fear" or "spreading false news" as a baseline to systematically erase valid human rights documentation and journalism from the digital history of Myanmar.
- **Cybersecurity Law (2025):** As the technical backbone of the digital dictatorship, this law regulates VPNs and mandates data localisation to force user traffic through State-controlled gateways. This grants the military's surveillance apparatus a comprehensive dataset of the population's online behaviour for behavioural analysis and threat detection.
- **Law Protecting the Privacy and Security of Citizens (2017):** In February 2021, the military suspended sections of the law removing the legal requirement for warrants before search and seizure, effectively legalising 24/7 digital surveillance and the interception of private communications without judicial oversight.

## International legal framework

In the absence of domestic protection, the rights of people in Myanmar must be viewed through the lens of international obligations and standards applying to both the State and technology companies.

- **International Covenant on Economic, Social and Cultural Rights:** Myanmar ratified the ICESCR in 2017. The State is bound to recognise the right to take part in cultural life and enjoy scientific progress. The military's use of AI to censor cultural expression and block the global internet via the Great Firewall directly violates these treaty obligations.
- **Convention on the Elimination of All Forms of Discrimination against Women:** As a State party, Myanmar is obligated to eliminate discrimination against women. The deployment of AI surveillance to facilitate the "dox-to-arrest pipeline" targeting women is a technology-facilitated violation of these commitments, amplifying gender-based violence.
- **UN Guiding Principles on Business and Human Rights (UNGPs):** In a conflict context where the State is the primary violator of human rights, the corporate responsibility to respect is paramount. However, technology companies operating in or supplying Myanmar are consistently failing to meet this standard. Specifically, they are neglecting to conduct Heightened Human Rights Due Diligence (HRDD) and are failing to perform adequate Human Rights Impact Assessments (HRIAs). By prioritising market access or cost-saving automation over rigorous safety checks, these companies risk complicity in the abuses committed using their technologies, such as the identification and subsequent torture of dissidents.

## Great Firewall as a weaponised divide

In Myanmar, the digital divide must be reframed not merely as a passive consequence of economic underdevelopment, but as a deliberate, State-imposed violation of the right to access information. The military has weaponised the country's telecommunications infrastructure to create a digital dictatorship, effectively severing the population from the global internet and, by extension, the benefits of the digital economy and cultural exchange. This constitutes a retrograde measure that directly contravenes the State's obligation to progressively realise the right to development.

This strategy relies on a comprehensive blacklist blocking system that fails the tests of necessity and proportionality required under international law for any restriction on freedom of expression. The military has coerced Internet Service Providers (ISPs) to block specific websites and platforms essential for communication and dissent, most notably Facebook, Instagram, X (formerly Twitter), and most independent news sites. By selectively banning these key platforms, which previously served as the primary entry point to the internet for most people, the military creates a discriminatory barrier that effectively isolates the population from information flows and resistance networks, while preserving connectivity for commercial elites.

This divide was formalised and hardened by the Cybersecurity Law enacted in January 2025. This legislation criminalises the tools necessary to bridge the divide, specifically regulating Virtual Private Networks (VPNs). Under this law, the establishment of a VPN is punishable by imprisonment and heavy fines. By criminalising the bridge to the outside world, the military has ensured that the digital divide is absolute, punitive, and fundamentally incompatible with the enjoyment of cultural rights.

### Impact on cultural rights and development

The imposition of this Great Firewall has had a catastrophic impact on the right to development, particularly in the sphere of cultural rights. Cultural development relies on the cross-pollination of ideas, access to diverse artistic expressions, and the ability to share one's own heritage and the world. The military's restrictions have rendered this participation impossible.

A stark example is the severing of access to independent media and educational resources. For students and academics, the military's VPN block acts as a barrier to the right to education, cutting them off from international research repositories, global news, and collaborative platforms essential for scientific and academic freedom. They are forced to rely on State-sanctioned curricula, which have been militarised and stripped of critical thought. This is not just a pause in development, but a regression, creating a knowledge vacuum where a generation is being raised in an information environment that violates their right to form opinions without interference.

Furthermore, the divide undermines the export of Myanmar's culture. Artists, filmmakers, and writers who previously used platforms like Facebook to exercise their right to freedom of expression and monetise their work have been silenced. Their digital distribution channels have been criminalised. The result is a forced cultural isolation where Myanmar's diverse voices, including those of ethnic minorities, are increasingly erased from the global stage, replaced entirely by the military's narrative.

## Risks and drawbacks of the digital dictatorship

The overarching risk of AI in Myanmar is the centralisation of arbitrary surveillance and the automation of repression. In a fragile State where the rule of law has collapsed, AI tools are not being used to enhance development, but to enforce a digital dictatorship. The military has integrated AI-powered technologies, specifically facial recognition and data processing systems, into its security apparatus to create a pervasive climate of fear. This transforms the public square (both physical and digital) from a space of cultural expression into a space of risk, effectively dismantling the right to participate in cultural life without fear of persecution.

### Algorithmic bias as structural exclusion

Algorithmic bias in Myanmar acts as a structural barrier to the right to non-discrimination in the context of development. Major AI models trained predominantly on Western datasets remain culturally and linguistically blind to Myanmar's diverse reality.

This bias manifests firstly as linguistic exclusion. Low-resource ethnic languages like Shan, Kachin, and Rakhine are underserved by AI tools for translation and moderation. This creates a discriminatory tier of development where digital benefits are accessible only to Burmese and English speakers, further marginalising minority cultural expression and undermining their right to use their own language.

Secondly, a pervasive engagement bias drives polarisation. As most clearly documented during the Rohingya crisis, social media algorithms favour content inciting anger or fear over peace-building. This design bias systematically amplifies hatred while burying cultural rights advocacy, actively undermining the State's obligation to prohibit advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence.

### Algorithmic silence and automated censorship

While State censorship is overt, AI-driven content moderation introduces a form of algorithmic silence that acts as an arbitrary interference with the right to freedom of expression. Social media platforms, which serve as the primary archive of Myanmar’s resistance history, rely on blunt AI tools to moderate content at scale. These algorithms often lack the cultural context to distinguish between violent content and documentation of war crimes.

Consequently, valid human rights evidence is routinely flagged and removed, or significantly down-ranked, effectively reducing its reach to near zero. This creates a reach gap where sanitised, pro-military propaganda spreads freely, while the harsh reality of the conflict, which is essential for historical truth, justice, and the right to remedy, is rendered invisible. This is not just a moderation error but is the erasure of a people's history by an automated system prioritising so-called safety metrics over human rights obligations.

### Chilling effects on cultural assembly

The military's deployment of the Person Scrutinisation and Monitoring System (PSMS) represents a profound threat to the entire cultural ecosystem of Myanmar. By integrating AI-enhanced facial recognition with cross-referencing capabilities (linking hotel guest lists, transport logs, and CCTV footage), the State has created a panopticon that extends far. This system effectively abolishes the concept of a safe public space necessary for cultural assembly. Whether it is a literary festival, a traditional performance, or a private gathering of artists, the knowledge that an automated system can instantly identify and profile every attendee creates a paralysing, chilling effect. Participation in cultural life becomes a high-risk activity, forcing artistic and cultural expression underground and dismantling the communal bonds that underpin Myanmar's diverse heritage.

## Disproportionate impacts on vulnerable groups

These digital risks are not distributed equally. They disproportionately target the most vulnerable, particularly women and ethnic minorities, amplifying pre-existing cultural inequalities and intersecting forms of discrimination.

For women, AI technologies have enabled a new, terrifying form of gender-based violence known as the "dox-to-arrest pipeline". Pro-military social media users, using AI-enhanced facial recognition on protest images, systematically identify women. Once identified, their personal details are published online (doxing) with explicit calls for their arrest or sexual assault. Furthermore, the rise of AI-generated deepfake pornography is being used to humiliate and silence women, effectively driving them out of the digital public square and stripping them of their right to participate in public life without fear of violence.

Ethnic and religious minorities, including the Rohingya, continue to face the lethal consequences of algorithmic negligence. Despite repeated warnings, social media platforms have failed to exercise human rights due diligence regarding the training of their content moderation AI. This blind spot allows hatred and incitement to violence to spread unchecked within these communities. The algorithm's failures mean that calls for harm can be amplified as engaging content, while counter-speech from these same minorities is suppressed or ignored, violating their rights to security of person and non-discrimination.

## Black box of cultural influence

The most profound long-term threat to cultural rights is the loss of cultural self-determination due to the opacity of AI systems. Myanmar faces a future where the public square is curated entirely by black box algorithms whose operations are invisible to the public. Because the code is secret, people cannot know why they see what they see, or conversely, why certain cultural movements remain hidden.

This lack of transparency poses a risk of algorithmic colonialism. If the algorithms shaping Myanmar's digital culture are optimised for engagement metrics defined by foreign corporations, or compliant with the censorship demands of the military regime, then the culture itself is being externally engineered. Small, invisible tweaks to a recommendation algorithm can silence an entire artistic movement or bury the history of a resistance struggle. Over time, this leads to a distorted historical record where people are unable to transmit their authentic culture to the next generation because the digital infrastructure that they rely on has been subtly rigged to exclude it.

## Failure of self-regulation

Self-regulation has proven demonstrably insufficient, particularly in conflict zones like Myanmar. Relying on technology companies to police themselves creates an inherent conflict of interest between profit and the corporate responsibility to respect human rights as outlined in the UN Guiding Principles on Business and Human Rights (UNGPs).

Firstly, the scale of AI operations renders manual oversight impossible, yet companies have consistently underinvested in safety teams for non-priority markets. Whistleblower disclosures have repeatedly shown that platforms are aware of their algorithms' harmful effects, such as amplifying divisive content, but choose to ignore them to preserve growth and engagement, failing their due diligence obligations.

Secondly, self-regulation fails to address the black box problem. Without external, binding obligations, companies have no incentive to be transparent about how their AI influences cultural discourse. Transparency cannot be voluntary but must be mandatory to ensure accountability.

## Institutional frameworks and the State as violator

In Myanmar, the institutional framework is not merely ill-equipped to protect rights. It is the primary instrument of their violation. The legal structures established by the military regime, such as the Cyber Security Law, are designed to weaponise digital infrastructure against the people, acting as a tool of repression rather than a safeguard. This represents a complete failure of the State's duty to protect human rights.

Concepts like data sovereignty, which in democratic contexts might protect people from foreign surveillance, are perverted in Myanmar to force tech companies to store data locally, where it can be seized by the military. Therefore, strengthening domestic institutional frameworks under the current regime would only empower the oppressor. Protection for Myanmar’s people cannot come from within the State currently. It must come from binding international mechanisms that hold both the military and the technology companies accountable to global human rights standards that cannot be legislated away by a local dictatorship.

## Conclusion

The intersection of AI and cultural rights in Myanmar is a battleground between creative resistance and digital dictatorship. While AI offers a fragile lifeline for anonymity and truth-telling, its current trajectory is overwhelmingly dominated by surveillance, censorship, and the automated erasure of dissent.

## Recommendations

- All States should enforce mandatory heightened human rights due diligence for technology companies operating in conflict zones like Myanmar. This must include specific requirements for companies to publish annual assessments of how their algorithms impact minority groups and political dissent.
- Establish a dedicated funding mechanism to provide support for victims of human rights violations caused by AI.
- Call for the creation of an independent, UN-backed auditing body to conduct mandatory algorithmic audits of major social media platforms in conflict settings and areas of gross and systematic human rights violations. This body must have the authority to access black box data to check systematic up and down-ranking.
- Immediately impose targeted sanctions on the supply of dual-use AI surveillance technologies (specifically facial recognition and predictive policing software) to the Myanmar military, classifying these exports as complicity in human rights abuses.