HUMAN RIGHTS MYANMAR

The effect of digital repression on transitional justice in Myanmar

Submission to the UN Special Rapporteur on Truth, Justice and Reparation – January 2026

Introduction

While new technologies offer unprecedented evidentiary tools for truth-seeking, the military's digital dictatorship currently serves as a primary barrier to transitional justice (TJ) by criminalising documentation, destroying digital memory, and facilitating digital negationism. This submission to the UN's review of new technologies and transitional justice highlights how digital technologies may both help and hinder efforts in Myanmar.

Opportunities and good practices

Technologies can contribute to the promotion of truth, justice, reparations, and guarantees of non-recurrence. The conflict in Myanmar has generated one of the most significant digital footprints in the history of human rights documentation. New technologies, when utilised by independent mechanisms and civil society, offer transformative potential for transitional justice.

Forensic justice at scale

The scale of atrocities in Myanmar, spanning thousands of villages and millions of victims, precludes traditional manual investigation alone. As noted in the Independent Investigative Mechanism for Myanmar (IIMM) 2025 Annual Report, the use of AI and machine learning to process over 28 million items of evidence has been groundbreaking. These tools allow for the identification of patterns of command responsibility, linking specific military units to burnings in Sagaing and Magway through the cross-referencing of satellite data and leaked internal communications.

Remote sensing and satellite forensics

High-resolution satellite imagery has allowed human rights organisations and other monitors to bypass the military's physical blockades. Satellite evidence has confirmed the destruction of thousands of civilian structures. This data provides a baseline for reliable information that the military cannot debunk as “fake news,” and it forms the empirical foundation for future reparations and restitution claims.

Verifiable citizen documentation

The future adoption of advanced verification, including blockchain-based and encrypted proof of life applications, by Myanmar’s civil society will increasingly allow for decentralised truth-seeking. Tools such as eyeWitness to Atrocities enable activists to capture metadata-rich footage that is cryptographically signed, ensuring that the chain of custody is preserved from the moment a crime is recorded.

Challenges and risks

There are many threats and challenges posed by new technologies to the pillars of transitional justice. In the hands of the military, technology is becoming a weapon of pre-emptive injustice. The 2026 election serves as a massive data-harvesting operation that now obstructs the path to accountability.

Digital negationism and AI-generated propaganda

The military is likely to be moving beyond simple disinformation to digital negationism. Using AI, the military’s information wing may have already produced deepfakes, including of opposition leaders of the National League for Democracy (NLD) confessing to corruption. This is likely to increase as tools become easier to access and the military’s skills improve. It will poison all evidentiary information and create benefits for disinformation campaigns, which will increasingly dismiss victims’ authentic testimonies as potential AI fabrications.

The documentation trap and PSMS

The military’s Person Scrutinisation and Monitoring System (PSMS), CCTV networks, and Deep Packet Inspection (DPI) tools reportedly use advanced technology, including perhaps facial recognition, to identify and locate people who work for civil society, including journalists and those documenting military movements. This system creates a documentation trap where the act of collecting truth-seeking evidence leads directly to arbitrary detention. Between 2021 and 2026, the proliferation of AI-powered CCTV cameras across urban centres is ending the era of anonymous so-called “citizen journalism”.

The “Great Firewall” and digital erasure

Through the deployment of Deep Packet Inspection (DPI) technology supplied by companies involved in China’s digital repression, the military has implemented an advanced system of interception. HRM’s report, *The Great Firewall of Myanmar*, outlined how systemic virtual private network (VPN) blocks prevent victims across the country, and particularly in rural areas, from accessing online reporting portals, uploading evidence to social media, or communicating with journalists or civil society groups. This results in the digital erasure of atrocities in real-time.

Intersectional impacts

New technologies affect women, youth, and ethnic minorities differently in the context of transitional justice.

Tech-facilitated gender-based violence (TFGBV)

The military utilises its digital dictatorship to enforce patriarchal control. As HRM noted in our report on *Sex-based violence in Myanmar*, military-affiliated Telegram channels use AI nudification to create non-consensual sexual imagery of women and women human rights defenders. This doxing is designed to create a reputational death, forcing women to withdraw from public justice and truth-seeking processes.

Ethnic information blackouts

In states like Kachin, Chin, and Rakhine, the military utilises strategic internet shutdowns to coincide with major ground offensives. These shutdowns are not merely about blocking communication but about ensuring that no digital evidence of war crimes and crimes against humanity survives. This creates a hierarchy of truth where urban crimes are documented while rural ethnic suffering remains invisible.

Youth surveillance and digital forensics

“Generation Z” activists are the military’s primary targets of mobile forensic tools during arbitrary checkpoint stops. By extracting contacts and encrypted chats, the military maps the entire social fabric of the resistance, ensuring that the next generation of truth-seekers is dismantled before they can participate in a future transitional justice process.

Role of private actors and business

Tech companies, including social media platforms, telecoms providers, and surveillance technologists, have responsibilities in the context of transitional justice.

Failure of heightened due diligence

Under the UN Guiding Principles on Business and Human Rights (UNGPs), companies must conduct “heightened due diligence” in conflict settings like Myanmar. However, domestic and foreign private companies have provided the infrastructure for the military’s DPI systems. Some social media companies have never conducted due diligence, and others conducted it previously but stopped. Furthermore, reports suggest that international investors continue to fund ISPs running networks with inadequate due diligence.

Algorithm accountability and “hate speech”

Social media algorithms continue to favour emotive and engaging content, which often includes state-sponsored propaganda, disinformation, and “hate speech” over civil discourse. In the lead-up to the military’s 2025-26 general elections, social media content amplified narratives that delegitimised ethnic groups and encouraged war crimes and crimes against humanity. Platforms must be held accountable for the real-world violence and changes in societal opinions facilitated by their algorithmic choices.

Preservation vs. deletion

A major challenge for future justice is the evidence deletion gap. Social media and other web platforms often remove violent content for violating community standards. However, they do not store this content. Without a mandatory international digital evidence preservation standard, vital records of war crimes and crimes against humanity may be permanently deleted from servers before mechanisms like the IIMM can subpoena them.

Institutional reform and non-recurrence

Measures and institutional reforms are needed to ensure new technologies support transitional justice and prevent recurrence. For transitional justice to be meaningful in the 21st century, the digital restoration of the State is as important as the reform of the judiciary.

Algorithmic audits and biometric de-listing

A future transitional government must include digital repression within any restoration process, such as a truth commission. This body would oversee the forensic audit of the military’s digital activities, including databases. Non-recurrence requires the right to be digitally forgotten by the State and any private actors, involving the destruction of biometric data harvested during the coercive censuses and elections.

Digital constitutionalism

Digital rights must be included in any future federal constitutions, grounded in the International Covenant on Civil and Political Rights (ICCPR) Article 17 (Privacy) and Article 19 (Expression). This must include a ban on the State’s use of mass facial recognition, and constitutional protection for the use of end-to-end encryption. It should also include legislative demilitarisation of the telecommunications sector.

Digital restitution

Reparations must include digital restitution, including the rebuilding of open, uncensored, and secure internet infrastructure in conflict-affected regions. Connectivity is a prerequisite for victims to access justice, reparations, and truth-telling platforms in the modern era.

Conclusion

The digital dictatorship in Myanmar represents a direct assault on the right to truth. The UN Special Rapporteur should consider including the following in their upcoming report.

Recommendations

- Global digital evidence preservation protocol: Call for an international standard requiring social media platforms to preserve, rather than delete, content flagged as potential evidence of atrocity crimes in Myanmar, ensuring it is accessible to independent judicial bodies.
- Moratorium on dual-use surveillance technology: Urge UN Member States to halt the export, sale, and transfer of facial recognition, DPI, and mobile forensic tools to the Myanmar military, identifying these as instruments of pre-emptive injustice that prevent the future guarantee of non-recurrence.
- Formalise digital restoration as a pillar of non-recurrence: Any future UN-supported transition frameworks for Myanmar must explicitly include the dismantling of the military's digital surveillance architecture and the restoration of user privacy through the destruction of illegally harvested biometric databases.