Myanmar's cyber law a serious threat to privacy, speech, and security

10 January 2025 – Issue 2

Rather than ensuring cybersecurity, Myanmar's newly adopted Cyber Security "Law" grants the military sweeping powers to control online spaces, enabling systematic violations of digital rights, including the rights to privacy, freedom of expression, and access to information.[1] This analysis highlights how the law deviates from international human rights standards and threatens privacy, digital security, VPN use, free expression, fair trial, digital rights NGOs, and social media.

While earlier drafts of the law under the National League for Democracy (NLD) administration already raised concerns about potential infringements on digital rights, post-coup revisions by the military in 2021 and 2022 further weakened safeguards. Human rights experts noted that the military's revisions added new crimes—some of which have now been removed—and stripped away protections. Therefore, this analysis compares the final adopted law to earlier drafts to examine how the military's repression has evolved.

Privacy protections removed

A fundamental aspect of cybersecurity is protecting individuals from privacy invasions, yet the Cyber Security Law contains no safeguards against State surveillance or misuse of personal data. Instead, the new law imposes disproportionate obligations on digital platforms, requiring them to retain user data for three years and hand it over upon mere request by any military-controlled authority, with the threat of temporary or permanent blocking for non-compliance (Arts. 33-34, 52).

Earlier drafts included privacy protections, but these were transferred to the 2021 amendment of the Electronic Transactions Law (ETL). This included privacy definitions (2022v Arts. 3.n–o), objectives (2022v Art. 4.c), duties (2022v Art. 14.i), and rules for data handling, unauthorised disclosure, and data destruction (2022v Arts. 79–81).

While it may seem positive that these provisions still exist elsewhere, by relocating privacy provisions to a separate law, the military has created legal uncertainty as enforcement becomes fragmented, increasing the risk of non-compliance and abuse. Authorities implementing the

[1] Civil society has declared that all "laws", "amendments", or derogations that are "adopted" by the military's State Administration Council are unlawful and unconstitutional under the 2008 Constitution.

Cyber Security Law may ignore or misinterpret privacy protections in the ETL. The Cyber Security Law also makes no reference to the ETL, failing to acknowledge privacy protections elsewhere. This omission could be deliberate, allowing authorities to argue that the Cyber Security Law operates independently from any privacy obligations in the ETL. Without an explicit legal link between the two laws, authorities could claim that the Cyber Security Law provides a standalone legal basis for surveillance, overriding any protections in the ETL.

By stripping away privacy safeguards and introducing vague, sweeping obligations for data retention, the final law facilitates mass surveillance, undermines individuals' right to privacy, and increases the risk of arbitrary interference by the military. It weaponises cybersecurity to expand State control, exposing individuals and vulnerable groups to cybercrime, abuse, and repression.

Security safeguards removed

The Cyber Security Law eliminates essential technical security safeguards, eroding digital trust and exposing Myanmar's digital environment to heightened cyber threats. Earlier drafts, including the military's 2022 version, identified protecting "electronic integrity" as a key objective (2022v Art. 4.g) and mandated authorities to develop and oversee electronic security (2022v Arts. 6.g, 20). Both provisions have been removed in the final adopted law.

Notably, the entirety of Chapter 8—which previously established standards for electronic communication and security—has been deleted (2022v Arts. 20–32). This chapter outlined critical measures such as electronic certifications and anti-hacking provisions (2022v Arts. 20–23). The absence of these safeguards undermines the right to security and leaves no clear framework to create reliable electronic systems, address digital fraud, or prevent unauthorised access.

Penalties for failing to protect critical infrastructure have also been significantly weakened. While the 2022 draft imposed penalties of up to three years in prison (2022v Art. 81), the final law reduces this to six months, signalling diminished accountability for ensuring digital security (Art. 60). Previous criminalisation of crypto-currency has been removed, but without adding protective regulations, further weakening safeguards against financial cybercrime (2022v Art. 95).

By removing these protections, the final law prioritises State control over ensuring public security, leaving critical systems vulnerable and exposing individuals to increased risks of exploitation and abuse. This systematic dismantling of security safeguards threatens the rights to remedy and security of person, further undermining trust in Myanmar's digital infrastructure.

VPN criminalisation partially removed

The Cyber Security Law appears to reflect a softened stance on individual VPN use, which is vital for accessing blocked platforms and independent news, supporting the right to freedom of expression and access to information. The military's 2022 draft criminalised VPN use, imposing

penalties of up to three years in prison (2022v Art. 90) and requiring vendors to obtain a license, punishable by up to one year in prison (2022v Arts. 62, 100).

In the final adopted law, penalties for individual use have been removed, focusing instead on unlicensed VPN vendors, with punishments including fines and up to six months in prison (Art. 70). This shift may indicate a response to business concerns, particularly from industries reliant on VPNs for secure operations and data protection, which align with the right to privacy and freedom from surveillance. It may also indicate that the military's deployment of advanced Chinese surveillance technology capable of blocking VPNs is sufficiently controlling digital activity, enabling mass surveillance and arbitrary interference with digital freedoms.

Freedom of expression criminalised

The new Cyber Security Law imposes vague, overbroad restrictions that violate the right to freedom of expression. Provisions require digital platforms like Facebook to censor content deemed to disrupt "peace", spread "rumours", disclose "unsuitable" information, or incite "terrorism", code in Myanmar for pro-democratic opposition groups (Arts. 31a-g). Failure to comply with these vague prohibitions results in penalties, including the potential blocking of the platform, turning providers into censors (Arts. 32, 52).

A new offence penalising the distribution of "information unsuitable for public viewing" threatens free expression with up to six months imprisonment (Art. 72). This vague clause risks criminalising dissent and restricting access to vital information. Similarly, a provision targeting "unwanted or unsolicited messages" with penalties of up to two years creates further risks, as it may be misapplied to legitimate communications and activism (Art. 68g).

The addition of a seventh criminal defamation offence to Myanmar's law books, punishable by up to two years (Art. 68f), perpetuates the military's ability to prosecute critics. This aligns with a long-standing pattern in Myanmar of using defamation laws to restrict digital freedom and silence dissent.

While some explicit offences from the 2022 draft, such as penalties for sharing sexually explicit content and spreading misinformation to cause panic, have been removed, these minor changes do little to address the law's overall chilling effect (2022v Arts. 91, 96). The broadly worded provisions signal an intent to tighten control over Myanmar's digital landscape, facilitating arbitrary enforcement and repression.

Undermining fair trial

The Cyber Security Law further undermines fair trial rights and due process, granting military-controlled bodies unchecked authority with minimal judicial oversight. One of the most alarming provisions is the assertion of universal jurisdiction, allowing the military to prosecute individuals globally for alleged cyberspace offences linked to Myanmar (Art. 3.a.2). This includes but does not appear to be limited to Myanmar citizens living abroad, and exposes exiled activists and journalists to significant risks (Art. 3.b).

Decision-making authority is concentrated in an unnamed government department (Art. 27a), with appeals adjudicated by a military-controlled committee rather than a court (Arts. 57-59). The department's power to impose severe penalties, such as fines, license revocations, or blocking, is broad and lacks transparency (Art. 51). These provisions expose individuals and entities, including digital platforms, to arbitrary rulings without meaningful recourse, violating the right to a fair hearing.

Additionally, the law grants the National Digital Laboratory final authority on electronic evidence (Art. 50b), denying defendants the right to challenge the validity of evidence—a cornerstone of fair trials. In a military-dominated system, this provision facilitates the use of fabricated evidence and politically motivated prosecutions.

By centralising power and dismantling safeguards for justice, the law deepens Myanmar's disregard for the rule of law. It denies fair trial rights and due process in the digital space, turning legal mechanisms further into instruments of political repression.

Digital rights NGOs at risk

The Cybersecurity Law requires providers offering cybersecurity services to obtain a special licence (Arts. 20-23, 28). However, the vague definitions of "vendor" and "services" (Arts. 4.h-j) create broad uncertainty, potentially including digital rights NGOs and CSOs, as well as individuals involved in digital security work, within the scope of the law. A special licencing regime for digital security allows the military to exert further control over civil society, threatening freedom of association.

Failure to comply with the law's obligations on licenced providers to submit reports (Art. 29) and cooperate on cyber threats (Art. 35) can result in severe consequences, including licence revocation and unspecified fines (Art. 51), imprisonment up to six months (Art. 62), and dissolution (Art. 53). Appeals are restricted to the military-controlled ministry and oversight committee, with no access to an independent judiciary (Arts. 54-59). These provisions create a chilling effect, hindering the operation of digital rights organisations.

Controlling social media

The Cyber Security Law imposes stringent regulations on domestic and international platforms, including global giants like Facebook, granting the military expansive control over social media. While enforcing these provisions on foreign platforms may be challenging, the law provides legal grounds for blocking or banning non-compliant platforms, facilitating censorship and arbitrary enforcement.

Platforms with over 100,000 users, whether local or foreign, must obtain a licence valid for three to 10 years (Arts. 24, 19). Licence approvals are managed by a government department, with appeals adjudicated by a military-controlled committee, bypassing judicial oversight (Arts. 25, 57-59). Although the military has removed an earlier requirement for platforms to host data on government-designated servers (2022v Art. 36.a), the law still empowers authorities to

inspect, suspend, take over, or ban platforms on vague grounds, often citing cybersecurity as a pretext for arbitrary actions (Arts. 42, 43a-c).

Additionally, platforms must identify, monitor, and remove content vaguely defined as disrupting “peace”, spreading “rumours”, disclosing “unsuitable” information, or inciting “terrorism”, which is code in Myanmar for pro-democratic opposition groups (Arts. 31a-g). Severe penalties for non-compliance, including blocking, grant the military sweeping powers to control online platforms, undermining freedom of expression and enabling the arbitrary restriction of platforms that resist its demands (Art. 52).

Conclusion

The military’s Cyber Security “Law” poses a grave threat to digital rights, including privacy, security, and freedom of expression. By dismantling safeguards and granting unchecked power to the military, it creates a framework for further surveillance, security breaches, censorship, and arbitrary action. Without urgent intervention, Myanmar’s digital space will remain a tool for repression.

Recommendations

- International community: Advocate for targeted sanctions against officials involved in implementing the law and ensure digital rights remain a priority in diplomatic engagements.
- Civil society: Provide technical and legal assistance to affected groups, including journalists and activists, to mitigate risks associated with increased surveillance and censorship.
- Tech sector: Resist compliance with provisions enabling censorship and surveillance, including by interpreting all orders narrowly to best protect human rights, while providing digital tools and support to circumvent online restrictions.
- United Nations: Review Myanmar’s Cyber Security Law through relevant mechanisms, such as the OHCHR, UN Special Rapporteurs on Myanmar, privacy, freedom of opinion and expression, and countering terrorism.