Regime's proposed Anti-Online Fraud Law targets dissent, not scams

8 June 2026

Introduction

While cyber-scam networks and trafficking compounds constitute a severe global crisis, the military regime's proposed Anti-Online Fraud Bill (May 2026) is not a genuine law enforcement measure. Instead, it functions as both a diplomatic smokescreen and a tool of further repression.

Globally, the military seeks to appear cooperative in addressing transnational cyber-scams and to appease mechanisms such as the Financial Action Task Force (FATF), aiming to avoid blacklisting and ease its access to international finance and investment. Yet the illicit cyber-scam industry is enabled by the military's own corruption, complicity, and the collapse of the rule of law, from which it profits.

Rather than dismantling criminal networks, the draft Bill serves as a cosmetic regulatory façade intended to mislead. Domestically, it further institutionalises mass surveillance, legalises arbitrary seizure of private assets, and expands the death penalty. It also functions as another security tool to monitor, target, and suppress human rights defenders, civil society organisations, media, and the political opposition using alternative networks to evade military control.

Legalising mass surveillance

The draft Bill further entrenches violations of the right to privacy in Myanmar by mandating real-time, centralised State access to private communications and financial data, and by effectively criminalising digital practices used to evade military surveillance.

Mandatory API integration

Article 57 requires private banks, telecommunications companies, and internet service providers (ISPs) to integrate their digital infrastructure directly with a State-run central network through Application Programming Interfaces (APIs). In practice, this compels private actors to build the technical pathways through which the State can access communications and financial data across sectors. The provision also requires those companies to bear the full costs of establishing and

maintaining the system, effectively conscripting the private sector into financing the infrastructure of State surveillance.

This is not a neutral technical requirement. By mandating direct system integration without independent oversight or any requirement of individualised suspicion, Article 57 creates the conditions for arbitrary interference with privacy rights.

Real-time tracking and database centralisation

Building on Article 57's mandatory integration requirement, the Bill establishes a centralised database into which private sector systems must feed, enabling the State to aggregate and access data from banks, fintech platforms, and telecommunications providers in real time.

Through this architecture, the State is empowered to monitor Internet Protocol (IP) addresses, SIM card usage, and financial transaction metadata, and to track financial activity on a continuous and indiscriminate basis, regardless of any individualised grounds or suspicion. Article 15 provides for the pooling and dissemination of information relating to financial flows and private communications.

Although Article 18 states that such information must be retained in accordance with "data protection standards", the Bill does not define those standards and creates no independent regulatory oversight or compliance mechanism.

Under international data protection principles, including those reflected in the GDPR, data protection without independent supervision is conceptually untenable. Under military rule, moreover, the regulator and the abuser are functionally the same. The result is a performative safeguard that serves to legitimise unrestricted State data harvesting, including against individuals involved in coordinating civil resistance.

The continuous aggregation of communications and financial metadata on this basis is incompatible with the principles of necessity and proportionality under international human rights law.

Mandatory data disclosure by telecommunications companies

In addition to the centralised surveillance architecture created through Articles 15 and 57, the Bill imposes direct and immediate data surrender obligations on telecommunications providers. Companies are required to retain comprehensive call detail records (CDRs), location data, and identity information, and to hand that information over immediately upon military demand, without judicial oversight.

The Bill secures compliance through criminal penalties that coerce private sector employees into functioning as agents of State policing. Under Article 40(c), telecom employees face up to seven years' imprisonment for failing to comply with, or delaying compliance with, non-judicial military requests. This framework compels employees to facilitate human rights violations under threat of punishment, directly engaging concerns of corporate complicity under Pillar II of the UN Guiding Principles on Business and Human Rights (UNGPs), and raising serious questions as to whether continued operations remain consistent with corporate human rights responsibilities.

Article 40(a) and (b) further criminalise the provision of services to unregistered SIM cards or to lines making an "unusually high" number of daily calls, punishable by up to seven years' imprisonment, while Article 34 imposes up to three years' imprisonment for registering a SIM card with incorrect details. These provisions directly target the secure and unregistered channels relied upon by underground activists and civil resistance networks.

Compelled disclosure without judicial authorisation, backed by criminal penalties, further entrenches arbitrary surveillance and coercive private-sector participation in rights abuse.

International legal assessment

This framework cannot be justified as an ordinary or proportionate response to online fraud. Under international law, any interference with privacy must be lawful, non-arbitrary, necessary, and proportionate (ICCPR, Article 17). Even where States pursue legitimate aims such as fraud prevention or cybercrime enforcement, surveillance measures must be narrowly tailored, subject to independent oversight, and limited to what is strictly necessary in the individual case.

The Bill does the opposite. Rather than authorising targeted measures based on objective grounds, it constructs a standing architecture of indiscriminate access, centralised monitoring, and compelled disclosure across the banking, telecommunications, and internet sectors. It dispenses with judicial authorisation and vests sweeping powers in a militarised Central Committee (Article 5), dominated by the Ministry of Home Affairs and its security apparatus.

In that context, the Bill is not a neutral regulatory response to digital crime. It is a legal and technical framework for repression, designed to convert anti-fraud governance into a system of mass surveillance capable of identifying, tracing, and punishing those who rely on digital tools to organise, communicate, and resist military rule.

Silencing digital dissent through "false" information offences

The military regime routinely invokes anti-cybercrime justifications to suppress freedom of expression, including independent journalism, digital activism, human rights documentation, and online efforts to challenge the regime's authority. This Bill further codifies those practices by criminalising vaguely defined speech, expanding censorship powers, and extending repression beyond Myanmar's borders.

Criminalisation of allegedly "false" information

Article 31 prohibits distributing or transmitting "false" information over a communication network for the purpose of committing fraud. In Myanmar's highly contested information environment, however, the military regime reserves the power to determine what is true or false. In practice, this enables the regime to characterise reporting on military atrocities, civil resistance activity, or online humanitarian coordination as "fraudulent" or deceptive.

This is not a narrowly framed anti-fraud provision. By relying on an undefined and inherently manipulable concept of "false" information, Article 31 creates broad scope for arbitrary enforcement against protected expression.

Website and social media blocking powers

Building on this vague speech restriction, Articles 14(d) and 14(e) empower the authorities to monitor, close, and block websites and social media accounts based on mere "suspicion" of criminal activity. Article 37 further requires ISPs to proactively block or remove access to any website the regime deems "fraudulent". Together, these provisions create an open-ended censorship framework capable of further targeting independent media, mutual aid platforms, and other forms of digital dissent.

Rather than requiring clear legal thresholds or independent review, the Bill grants sweeping discretion to suppress online content before any wrongdoing has been established. This sharply departs from the principle that restrictions on expression must be exceptional, necessary, and subject to adequate safeguards.

Extraterritorial jurisdiction

The Bill also extends the military's repressive framework beyond Myanmar's territory by explicitly asserting jurisdiction over Myanmar citizens, including diaspora activists, and permanent residents living abroad. This extraterritorial reach enables the military to criminalise, monitor, and prosecute online dissent conducted overseas, including cross-border humanitarian coordination and international advocacy undertaken in response to the crisis in Myanmar.

By projecting vague cybercrime provisions across borders, the Bill seeks to chill protected expression and association not only inside the country but also among communities abroad who document abuses, support resistance networks, or mobilise international attention.

International legal assessment

International human rights law requires restrictions on expression to be clearly and narrowly formulated so that individuals can regulate their conduct accordingly (ICCPR, Article 19; Human Rights Committee, General Comment No. 34). Terms such as "false" information are inherently broad and highly vulnerable to arbitrary interpretation, particularly in a context where the State itself is the principal source of repression and disinformation.

The Bill fails that standard. Rather than addressing cyber-enabled fraud through precise and proportionate measures, it equips the military with a legal basis to criminalise contested speech, censor digital platforms on suspicion alone, and extend repression to critics and activists abroad. In the context of Myanmar's ongoing conflict, these provisions operate not as legitimate regulation but as tools to dismantle digital political opposition, punish reporting on military abuses, and obstruct online humanitarian and advocacy efforts.

Dismantling due process in financial enforcement

A central feature of civilian resistance to the military coup has been the rejection of the regime-controlled formal banking system in favour of mobile wallets, informal hundi payments, and cryptocurrency to support civil disobedience, humanitarian relief, and mutual aid. This Bill is designed to disrupt those alternative financial routes by enabling rapid freezes, compelling bank-led enforcement, and denying meaningful avenues of challenge or remedy.

Emergency account freezes and asset deprivation

The Bill authorises the immediate freezing of accounts within 15 minutes of an "emergency" report and permits banks to hold funds for up to 72 hours without prior judicial authorisation. In practice, this creates a mechanism for the rapid disruption of crowdfunding for emergency relief, strike support, and other forms of civilian assistance, particularly where speed is essential.

This is not a narrowly supervised emergency power. By permitting deprivation of access to funds on an accelerated timetable and without prior judicial review, these provisions create clear scope for arbitrary interference with property-related interests and due process rights.

Account suspensions based on "unusual" transactions

The Bill further requires banks to freeze accounts unilaterally when they detect "unusual" financial flows, allowing customers to be deprived of access to their assets before any charge is filed or wrongdoing established. In the current context, routine transfers to mutual aid networks, displaced families, or resistance-linked support structures are readily liable to be treated as suspicious.

By using vague indicators such as "unusual" activity without clear legal thresholds or independent oversight, Article 26 turns ordinary financial behaviour into a basis for pre-emptive punishment. It thereby undermines the presumption of innocence and normalises punitive financial restrictions in the absence of adjudication.

Coercive duties imposed on financial institutions

The Bill also weaponises the banking sector by coercing financial professionals into acting as instruments of State surveillance and repression. Under Article 38, bank officials face up to seven years' imprisonment for failing to investigate or report "suspicious" financial activities. This places financial workers under threat of criminal punishment unless they actively identify and report transactions deemed suspect by the regime, including efforts to move funds outside military-controlled channels.

Article 60 compounds this framework by granting effective impunity to those carrying out arbitrary account freezes, expressly barring civil or criminal litigation against financial officials for actions taken under the law. Victims are thus stripped of any meaningful domestic avenue to challenge wrongful asset seizures, while financial institutions are insulated from accountability for participating in abusive enforcement.

Together, these provisions transform banks from service providers into coercive arms of State control. They also raise serious concerns of corporate complicity, particularly for financial actors participating in arbitrary and unreviewable restrictions on access to funds.

International legal assessment

These provisions are incompatible with core due process guarantees under international human rights law. Article 14 of the ICCPR protects the right to a fair hearing by a competent, independent, and impartial tribunal and reflects the broader principle that punitive measures should not be imposed absent lawful process and the presumption of innocence. Article 2(3) further requires an effective remedy for rights violations.

The Bill moves in the opposite direction. It permits rapid account freezes without prior judicial authorisation, encourages deprivation of assets based on vague indicators of suspicion, coerces bank officials into enforcing State repression, and bars victims from seeking civil or criminal redress. In substance, it replaces adjudication with administrative coercion and converts financial regulation into a mechanism for punishing and disabling civilian resistance. In the context of Myanmar, these are not ordinary anti-fraud powers, but tools for dismantling the financial channels on which humanitarian support, mutual aid, and political opposition depend.

Imposing the death penalty for economic offences

The Bill introduces extreme and grossly disproportionate punishments that are wholly detached from ordinary international criminal justice standards. In the context of Myanmar, these provisions function not as legitimate anti-crime measures, but as a tool of terror against those involved in parallel economic activity, alternative financial networks, and other forms of resistance to military rule.

Capital punishment for economic and online offences

Articles 53 and 54 permit the death penalty for a broad range of offences linked to so-called online fraud, including operating online fraud centres (Article 44), digital currency fraud (Article 45), recruitment for online fraud (Article 46), violence or detention connected to online fraud (Article 47), labour exploitation (Article 48(a)), and human trafficking (Article 48(b)).

Although some of these offences may involve serious criminal conduct, the Bill places different forms of behaviour into a single punitive framework and exposes defendants to capital punishment far beyond the narrow limits recognised under international law. In particular, extending death eligibility to offences such as digital currency fraud or recruitment-related conduct radically departs from the principle that punishment must be proportionate to the gravity and nature of the crime.

In Myanmar's current context, where the regime routinely characterises oppositional or informal economic activity as criminal, these provisions create a legal pathway for imposing the harshest possible punishment on individuals associated with unauthorised financial systems or parallel civilian structures.

International legal assessment

International law strictly limits the death penalty to the "most serious crimes", understood as crimes of extreme gravity involving intentional killing (ICCPR, Article 6(2); Human Rights Committee, General Comment No. 36). Offences such as digital currency transactions, operating unauthorised online businesses, or recruitment-related offences do not meet that threshold.

The Bill, therefore, violates the substantive limits imposed by international law on capital punishment. That violation is even more acute in Myanmar, where the absence of judicial independence and due process means that any death-eligible offence is embedded in a system structurally incapable of delivering fair and reliable adjudication. In that context, these provisions do not simply prescribe disproportionate penalties; they create a legislative mechanism through which the military can legally execute individuals involved in alternative financial networks, informal governance structures, or other forms of resistance under the guise of anti-fraud enforcement.

Conclusion

The Anti-Online Fraud Bill is not a genuine public safety measure. It is a repressive security instrument that uses the language of cybersecurity and transnational crime to legitimise mass surveillance, censorship, financial coercion, and extreme criminal punishment under military rule. Rather than addressing online fraud through targeted and proportionate means, it creates a legal framework for monitoring private communications, disrupting alternative financial systems, criminalising digital dissent, and insulating abusive enforcement from challenge.

Its practical function is therefore not the eradication of cybercrime, but the dismantling of the digital and economic pathways through which people in Myanmar have sought to protect themselves, organise resistance, deliver humanitarian support, and circumvent military control.

As one of the first major legislative drafts advanced by the "new" government made up of former military commanders, the Bill is also politically significant. It signals a deeply regressive governance agenda in which digital autonomy, financial self-organisation, and civic resistance are treated as threats to State security. In doing so, it further confirms that the military's priority is not the protection of the public but the consolidation of coercive control.

Recommendations

- **Myanmar military regime:**

  Withdraw the Anti-Online Fraud Bill in its entirety. Any response to online fraud should be grounded in legality, necessity, proportionality, and independent oversight, and must not be used to expand surveillance, criminalise expression, or punish the use of alternative financial and digital networks.

- **International governmental organisations, diplomatic missions, international financial institutions, and foreign and international police:**

Publicly reject the Bill as incompatible with international human rights standards and avoid any engagement that could legitimise it as an ordinary anti-fraud measure. Governments should make clear that efforts to address cyber-scams and transnational organised crime in Southeast Asia must not be used to strengthen Myanmar's military surveillance, censorship, or financial repression apparatus. They should also warn domestic telecommunications, technology, and financial institutions of the legal, human rights, and reputational risks of complying with abusive measures under the Bill.

- **Private telecommunications, technology, and financial companies**

  Conduct urgent human rights due diligence, including Human Rights Impact Assessments, in line with the UN Guiding Principles on Business and Human Rights. Companies should refuse, to the maximum extent possible, compliance with measures that require direct system integration, arbitrary data disclosure, censorship, account freezing, or other forms of participation in rights abuse. Where severe legal coercion makes meaningful mitigation impossible, companies should assess whether continued operations are consistent with their human rights responsibilities and prepare for a responsible exit where necessary.