Myanmar: Note on New Draft Cyber Security Law

April 2022

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction[1]

In February 2021, the military regime running Myanmar circulated a draft Cyber Security Law. The Centre for Law and Democracy (CLD) prepared an analysis of that draft on an urgent basis with a view to helping local stakeholders understand the problems with it from the perspective of international human rights law.[2] Following a barrage of criticism, the military regime appeared to withdraw the draft Cyber Security Law that same month. However, a revised draft was circulated in January 2022 (draft Law). This Note provides an analysis of the new features of the draft Law (i.e. the January 2022 version).[3] As such, it should be read in conjunction with our earlier Analysis. Like that Analysis, the focus of this Note is on the human rights implications of the draft Law, with a particular focus on freedom of expression. As such, it does not address a number of other potential problems such as practical challenges in implementing it or the costs involved.

We note, at the outset, that all of the concerns we expressed in our February 2021 Analysis remain relevant. A few of the most significant concerns outlined in that assessment were:

[2] That Analysis, along with other work we have done relating to Myanmar post military coup, is available on our Myanmar Resource Page at https://www.law-democracy.org/live/legal-work/myanmar-resource-page/. The Analysis itself is available at: https://www.law-democracy.org/live/wp-content/uploads/2021/11/Myanmar.Cyber-Security-Analsyis.Feb21-1.pdf.

[3] Our analysis is based on an unofficial translation of the draft Law. We note that in many places the translation is unclear and hard to understand. We apologise for any errors in our analysis based on unclear translation.

- Very significant powers, including regulatory powers over freedom of expression and the power to impose sanctions, are allocated to bodies such as the Central and Steering Committees which are not independent of the military regime, the exercise of those powers is not subject to appropriate either procedural or substantive constraints, and the decisions of those bodies are not subject to court review.
- Broad-ranging and vaguely-worded restrictions on the content of what may be disseminated online are imposed (and applied by the bodies noted above).
- A number of other (i.e. beyond content) criminal offences are created which are again vague, are repetitive with only minor linguistic differences between provisions, and lack the appropriate (and specific) intent requirements that would be needed to justify such prohibitions.
- A number of onerous obligations are imposed on digital service providers, defined very broadly, as well as sub-sets of that broad category (such as "cyber security service providers"), some of which are clearly designed to further military control of digital communications, some of which are unreasonably burdensome for service providers and many of which simply fail to take into account the working reality of international service providers.
- The scope of special obligations ostensibly designed to protect critical information infrastructure is far too broad both in terms of the way that infrastructure is defined and the bodies which may be deemed to be subject to these rules.

Our February 2021 Analysis also included a critique of the rules in the February 2021 version of the draft Law on personal data protection. These rules have been retained, essentially verbatim, in the current version of the draft Law. We note that these rules are already part of the current legal framework of Myanmar as they were included, again essentially verbatim, in the amendments to the Electronic Transactions Act (ETA) which were introduced in February 2021.[4] While the current draft of the Cyber Security Law would repeal the ETA, it remains the case that this is a fundamentally limited set of protective rules on personal data protection, while other rules in the draft Law require this data to be stored locally and to be retained for "up to three years" (which we understand as meaning for three years), both of which are not legitimate under international law, as well as to be shared with an "assigned person or authorised organisation requested under any existing law", without adequate protections for this being put in place.

[4] Those amendments were introduced around the same time as the February 2021 draft Cyber Security Law was withdrawn and were drawn directly from that draft Law.

The rest of this Note focuses on new concerns based on revised provisions in the current, January 2022 version of the draft Cyber Security Law.

Institutional Structures

As noted above, we already had very significant concerns with the institutional structures and the powers they wield based on the original draft version of this Law. These concerns have become even more problematical with the current proposed amendments. The powers of the Central Committee, firmly under the control of the military regime, have been expanded in two key areas, both of which relate to other concerns which are noted below. The first, set out in Article 6(j) of the draft Law, gives the Central Committee the power to establish the National Digital Laboratory which will play a key role in approving electronic evidence for court consideration. The second, set out in Article 6(k), grants the Central Committee the power to set out policy, rules, regulations and directives, in coordination with the Central Bank of Myanmar, for online financial services.

Another concern is the significantly expanded provisions on electronic certification and licensing of bodies to "operate as an authorised electronic certification issuer" (i.e. to act as a trusted issuer of digital certificates so that third parties may rely on those certificates when used by their subjects or owners, a key foundation of trustworthy electronic commerce). These rules are to be undertaken by a body variously described in English as the "Electronic Communications Supervision Committee", the "Electronic Communications Supervision Working Committee" and the "Electronic Certification Authority".[5] Article 3(u) defines the latter as "an authorised person to validate the authenticity and integrity of an electronic or digital certificate", but how this body would be created is not defined in the draft Law (although the Steering Committee, with the approval of the Central Committee, creates the Electronic Communications Supervision Committee). Previously, this area of regulation was conducted by the "Department" which, in turn, was the secretariat of the Central Committee. Thus, while this area of regulation would already have been under the control of the military regime according to the original version of the Cyber Security Law, the rules and institutional structures governing it have been significantly expanded in the current version.

Virtual Private Networks

[5] It is not entirely clear to us whether these are two or three different bodies or just one body.

A very important new development in the draft Law is the attempt to bring the use of virtual private networks or VPNs under the control of the military regime. A new Article 62 provides that to set up a VPN (or to use similar technology) on a licensed network (i.e. to use one on your Internet or mobile plan), you must first apply to the Ministry for permission. In other words, using a VPN over a local communications network is illegal absent Ministry permission. According to Article 90, a failure to respect this rule shall be punished by between one and three years' imprisonment (i.e. a minimum of one year's imprisonment), a fine up to five million MMK (approximately USD 2,700) or both.[6] Furthermore, various other provisions cover ancillary offences which might be deemed to relate to this, such as Article 89(c), which makes it an offence to encourage or assist someone to access a cyber source in violation of the law.

This is clearly contrary to international law, which protects the rights to use anonymisation and encryption tools, including VPNs. As a practical matter, VPNs have become a lifeline for many people in Myanmar who are simply trying to exercise their rights to freedom of expression whether by expressing themselves or by accessing information provided by others.[7]

Content Restrictions

As noted above, the February 2021 version of the draft Law already included extensive and illegitimate restrictions on the content that could be accessed and shared digitally – banning such content as "misinformation and disinformation" and even "written and verbal statement against any existing law" – and then required Internet service providers to remove this content. The very problematical existing rules have all been preserved in the current version of the draft Law and one more has been added, namely for content which may damage an individual's social standing and livelihood (Article 35(f)). While it is legitimate to provide for appropriate protection for individuals' reputations, via a defamation law, the Myanmar legal framework already provides more than sufficient protection for this.[8] Thus, there is no need

[6] According to some sources, the authorities are already cracking down on the use of VPNs, even though the legal basis for this is not clear. See Frontier Myanmar, Daily Briefing, "VPN crackdown begins", 27 January 2022.

[7] VPNs have, for example, become essential tools to access Facebook, among other services, since the military ordered telecommunications service providers to block access to it shortly after the coup. For more information about the rise in VPN usage in Myanmar, see Beh Lih Yi, "The military has imposed information blackouts as people turn to VPN and encrypted messaging apps to skirt restrictions", 25 February 2021, https://news.trust.org/item/20210217141412-ljfpg.

[8] See Joint submission to the Universal Periodic Review of Myanmar by Arakan Journalists Association, ARTICLE 19, Athan, Centre for Law and Democracy, Free Expression Myanmar, Generation Wave, Kachin State Youth Assembly, Karen Human Rights Group, Karenni National Youth Organization, Myanmar Centre for Responsible Business, Myanmar ICT for Development Organization, Myanmar Journalist Network, Myanmar Media Lawyers'

to expand this protection. In any case, Article 35(f) not only signally lacks the protections that are required to make defamation laws legitimate under international law, but it also provides for criminal penalties for breach, again contrary to international law.[9]

Financial Measures

As noted above, the Central Committee is now empowered, in coordination with the Central Bank of Myanmar, to set out policy, rules, regulations and directives for online financial services. Current Article 94 (formerly Article 66) makes it an offence to provide online financial services without being legally registered in Myanmar and absent permission from the Central Bank of Myanmar, subject to imprisonment of between one and three years (formerly just up to three years) and/or a fine of up to ten million MMK (approximately USD 5,300). A new Article 95 specifically creates the offence of buying or selling "illegal currency such as digital currency, cryptocurrency" online, subject to imprisonment of between six months and one year and/or a fine of up to 25 million MMK (approximately USD 13,300).

It is not illegitimate for countries to impose reasonable regulations on the provision of financial services and the use of cryptocurrencies. We are not aware of what sorts of specific regulations in this area may already have been put in place, although there seems to have been some debate about whether cryptocurrencies were illegal even before the coup.[10] However, the adoption of the Cyber Security Law in its current form would presumably clarify that these currencies are illegal. Furthermore, with the increasingly strict rules being put in place by the military regime governing financial transactions in general, including in relation to foreign currency,[11] the aim of these measures is clearly to extend control by the regime over all aspects of civic life in a manner which represents a clear breach of the right to freedom of association.

Network and Progressive Voice, 9 July 2020, paras. 4-7, https://www.law-democracy.org/live/joint-submission-to-the-universal-periodic-review-of-myanmar-raises-freedom-of-expression-concerns/.

[9] Formally, there is no specific criminal penalty in the current draft of the Law for breach of Article 35, which contains all of the content restrictions, including this one, but see the note on this under Offences, below.

[10] See, for example, Turner Wright, "Myanmar Central Bank Claims Crypto is Banned, Users Disagree", 22 May 2020, suggesting that while the Central Bank of Myanmar claimed that cryptocurrencies were illegal, others disputed this. See https://cointelegraph.com/news/myanmar-central-bank-claims-crypto-is-banned-users-disagree.

[11] See Elaine Kurtenback, "Military-led Myanmar seeks to reassure foreign investors", 21 April 2022, https://apnews.com/article/business-myanmar-united-nations-embassies-b6166f8a17ddb59dd3967b3ed67cbeb1.

Evidence

Two new provisions on evidence, combined with the power of the Central Committee to establish the National Digital Laboratory, are also of concern. Article 66 provides that if "the evidence relating to an offence filed under this law is not easy to bring to court, it can be presented with a report or other relevant documentation on how the evidence is kept without going to court." In this case, the evidence is deemed to have been presented legally before the court and the court shall act accordingly. Importantly, pursuant to Article 67, if any dispute arises regarding the submission of electronic evidence, the National Digital Laboratory shall have the power to make the final ruling on the matter.

This is highly problematical. While it is not yet clear how the National Digital Laboratory will be constituted, the whole approach of the draft Law, not to mention the wider approach of the military regime, very strongly suggests that this body will not be independent of the regime. As a result, this will create a situation where the regime, which will very often be one of the parties to a dispute before the courts, effectively gets to dictate what evidence may and may not be accepted. This runs directly contrary to the whole principle of the rule of law both in terms of parity of parties before the courts and in terms of the courts being independent and able to control their own processes.

Offences

A number of important changes have been made to the provisions on offences in the draft Law. A whole new Chapter 15: Administrative Actions has essentially replaced one provision, Article 72 in the February 2021 version. The latter allowed the Department, the secretariat of the Central Committee, with the approval of the Steering Committee, to warn, impose a fine on, or suspend or revoke the service or licence of any party which failed to respect Articles 44 or 48 (now Articles 44 and 58) providing, respectively, for online service providers to cooperate with the various committees tasked with responding to cybercrimes and attacks and for telecommunications service providers to collaborate with those who had been authorised to intervene under existing laws (the scope of this was never clear).

Pursuant to Chapter 15, these administrative provisions have been very significantly expanded. Bodies which are authorised to issue electronic certificates may suspend or cancel those certificates for any breach by the certificate holder of the law (Article 69). If, in turn, a body which is authorised to issue electronic certificates is in breach of the law, the Electronic Communications Regulatory Committee may impose a fine or suspend or cancel their licence (Article 70). Articles 71-73 grant the Department, with the approval of the Steering Committee,

the power warn, impose a fine, or suspend or revoke the service or licence of relevant bodies – namely digital, cyber security or telecommunications service providers – for breach of Articles 34, 36, 54 and 58 (which cover a range of issues such as meeting technical standards, being prepared for cyber attacks, paying taxes and collaborating with the various cybersecurity bodies), and also arguably Article 35 (on content restrictions).

Given that the Department and Steering Committee, and presumably eventually the Electronic Communications Regulatory Committee (which is not directly provided for in the draft Law, as noted above), are all fully controlled by the military regime, and hence lack independence from the de facto governing authorities in the country, granting these bodies the power to sanction bodies the operations of which underpin expressive activity on the part of citizens and residents is simply not legitimate.

Furthermore, appeals from these decisions go, in the case of a decision by a body which is authorised to issue electronic certificates (as provided for in Article 69), to the Electronic Communications Regulatory Committee (pursuant to Article 75), and in other cases (as provided for in Articles 70-73) to the Central Committee (pursuant to Articles 76-77). The decision of the Central Committee is then final (Article 78). As such, not only are important sanction decisions made at both the initial and appeal levels by bodies which are not independent, but the jurisdiction of the courts to review these decisions is ousted.

Whereas Article 61 of the February 2021 version of the draft Law provided generally for criminal penalties for online service providers which failed "to comply with the provisions prescribed in this Law", that general rule has been removed in the current draft Law and there is presently no specific criminal penalty for breach of Article 35, which contains the content restrictions. Some of the provisions under Article 35, such as spreading mis- or disinformation or spreading sexually explicit content, are the subject of specific sanctions (for these two provisions, respectively, through Articles 90 and 96). And, pursuant to Article 89(c), it is a crime to encourage or assist in giving access to a "cyber source" in violation of the rules, which could be used to enforce Article 35 as well. Article 71, providing for administrative penalties, does reference Article 35 although, at least in English translation, it does not clearly provide for penalties to be imposed for breach of this article. We assume that what is presumably an "oversight" (i.e. lack of a general enforcement provision for Article 35) will eventually be remedied if and when the draft Law is further considered by the military regime.

The introduction of minimum sentences of imprisonment, mentioned above, is new in the current draft Law (i.e. these were not present in the February 2021 version) and these now apply very widely to Articles 84-88 and 90-100. Formally, all of these provisions provide for

imprisonment "or" a fine, and so are technically not mandatory minimum imprisonment sentences. However, it seems very likely that they will in practice be treated in that way. Providing for minimum mandatory periods of imprisonment is, outside of more serious offences, not legitimate as it fails to accommodate the principle that the sentence should correspond to the gravity of the wrong done. This is especially true given the wide range of actions which could constitute a breach of any of these articles, many of which may represent very minor wrongs. And even providing for minimum mandatory periods within a sentence of imprisonment (which, technically is what these articles do), is distinctly not better practice as, again, it mitigates against the sentence reflecting the gravity of the wrong done.

In line with a number of legal amendments introduced by the military regime, there are also two new security-related offences. Article 92 creates a special crime where various cyber-offences, such as hacking or inserting malware, attract more serious sanctions – namely between two and five years' imprisonment and/or a fine up to 30 million MMK (approximately USD 16,000) – where they are done "with an intent to threaten or disturb national sovereignty, security, peace and stability, rule of law and national solidarity". It is significant that security and peace are lumped together here with national solidarity. Article 93 covers various cybercrimes committed with the "intent of deteriorating the relationship between the country and other foreign countries or for the interests of other foreign country" and provides for even more onerous sanctions, namely between three and seven years' imprisonment and/or a fine up to 50 million MMK (approximately USD 27,000).

While it is not necessarily illegitimate to provide for harsher penalties where crimes are committed with these sorts of intent, Myanmar already has sufficient rules to protect national security online.[12] And, as noted earlier, these rather harsh minimum prison sentences are very suspect given the range of actions that could potentially trigger a conviction under these provisions.

Recommendations

The Centre for Law and Democracy usually makes detailed recommendations based on each specific critique it has made of a law or draft law. However, this Note only reviews the amendments to the draft Law rather than all of the problems with it. That, and the very

[12] See, for example, Centre for Law and Democracy, "Myanmar: Groups Plan to Reform Digital Content Restrictions", 10 December 2017, https://www.law-democracy.org/live/myanmar-groups-plan-to-reform-digital-content-restrictions/.

fundamental problems with this draft Law, mean that our only recommendation at this time is that the whole idea of the military regime introducing this law should be dropped. At such point as a democratic government returns in Myanmar, proper consultations could be held as to what form of cyber security law might be needed.