ALLEN & OVERY

Update from on the ground: Draft Cyber Security Law – Implications for business in the ICT sector in Myanmar

1. Introduction

On the morning of 1 February 2021, in response to allegations of voter fraud, Vice-President Myint Swe (who has since assumed the role of acting President) declared a State of Emergency for one year and conferred full legislative, administrative and judicial power to Senior General Min Aung Hlaing, the Commander-in-Chief of Myanmar's armed forces.

This article forms part of an ongoing series of updates on key developments in Myanmar and their implications for investors into the country. This update focuses on the recently released Cyber Security Law bill issued by Myanmar's new military regime, in particular on the implications for online businesses and infrastructure providers relevant to the ICT sector in Myanmar.

2. Background

The military regime released a draft Cyber Security bill (the **Draft Law**), with the objectives of securing cyber systems, critical information infrastructure, and personal data, safeguarding against and managing cyber attacks, and supporting the digital economy. The Draft Law was released to telecommunications operators and internet service providers on 9 February 2021 with a request to respond within a very short period by 15 February 2021.

The Draft Law has been criticized by many civil society groups inside and outside Myanmar, which issued a joint statement on 10 February 2021, expressing their concerns with the bill from privacy and other human rights perspectives.

The military regime has already issued orders for internet blockouts – first on 1 February and again on 6-7 February, and has undertaken to restrict access to certain online media by issuing take down orders to telecommunications operations and internet service providers. Commentators have widely observed that the military regime has sought to strengthen its control over online communications and media within Myanmar with the rapid issuance of this Draft Law.

3. Impact on business

We have set out below some of the key issues with the Draft Law impacting business operating in or relevant to the ICT sector in Myanmar.

3.1 Critical Infrastructure Providers

The Draft Law sets out a framework for the protection of "Critical Information Infrastructure", which is defined broadly to include electronic information and infrastructure related to: eGovernment, finance and budgeting, water resource, transportation, communication, public health, electricity and energy and natural resources, and any such infrastructure that is not for public use.

This definition is further subject to amendment by the Administration Council, introducing a level of uncertainty in future application.

The Draft Law stipulates that the Steering Committee shall have inspection rights on the cyber security of critical information infrastructure, that any "information on critical information infrastructure" must be stored at an authorised location, and such information may only be dealt with (transferred, shared, used etc.) in accordance with as yet undefined regulations. In addition, a cybersecurity report must be submitted by operators of the critical infrastructure in on a yearly basis.

Businesses falling within the definition of Critical Information Infrastructure should consider their ability to satisfy these requirements – in particular any data localisation requirements prescribed by the Ministry, and consider the potential operational impact of the steering committee restricting the transfer of such information within or outside of Myanmar.

3.2 Online Service Providers

The Draft Law sets out obligations and restrictions applying to "online service providers", defined broadly to capture persons or businesses which provide services used in Myanmar through a network, a computer or other kind of communication device. We have set out below elements of the Draft Law that are most relevant to participants in the ICT sector in Myanmar that may fall within the definition of online service providers.

(a) Registration

The Draft Law mandates that all online service providers must be licensed to operate within Myanmar by a yet to be established "steering committee" within one year of the Draft Law being enacted. Without a definition of the frameworks or policy under which licences are to be granted, the steering committee will have effective control over the online businesses able to operate in Myanmar (including over those currently operating) and creates additional administrative burden for online business servicing the country (regardless of whether they are local or overseas based). Furthermore, all online service providers are required to incorporate under Myanmar Companies Law and be subject to taxation laws – which presents additional challenges for businesses that aren't incorporated or adopt other legal structures (for example, individuals selling goods online via social media, or partnerships).

This licencing regime in its current form is likely to apply to internet service providers in Myanmar, which are separately regulated by telecommunications law – it remains to be seen how this overlap is addressed.

Businesses operating in Myanmar should consider whether some or all of their operations could fall under the online service provider definition. The broad discretion of the steering committee in granting licenses to operate presents a risk to current and prospective online-based businesses in the country.

(b) Data localisation

Online service providers and internet service providers must ensure that devices storing "user information" are located at an authorised location, and specified information (including usernames, IP addresses, ID numbers, contact details and user records) are retained for a period of three years from a user's first use of the service.

As this effectively requires online service providers to establish data storage capabilities within Myanmar, this requirement presents challenges to foreign-based online service providers such as Facebook or Amazon Web Services who are unlikely to maintain a local presence, and may act as a barrier to entry for new online services being launched in Myanmar.

Whilst data localisation and retention requirements are unlikely to apply to all of the data an online business holds or uses, reference to "user information" is broad, and so all online businesses operating in Myanmar will need to consider how compliance can be operationally achieved and managed, depending ultimately on the data storage locations specified by authorities.

(c) Inspection

The Draft Law provides for a broad right for the Ministry to "investigate and supervise" any online service provider and access their records if necessary for "countries protection and security purposes and public interest".

This is a broadly framed right of means that online businesses may be subject to random inspection by authorities.

(d) Suspension, termination of operations

The Ministry has the right, for reasons of "public interest" to temporarily suspend or control devices of an online services provider, or permanently terminate an online services provider in Myanmar. The Draft Law does not require an emergency for this right to be exercised, and there is no further guidance on the definition of "public interest".

As currently framed, this right to terminate or suspend online service providers may be exercised arbitrarily with reference to a "public interest" – this presents a risk to current and prospective online businesses in Myanmar.

(e) Content controls

Online service providers are required to prevent, remove, delete or suspend a wide range of content upon the instruction of the Ministry, including content deemed to be "misinformation and disinformation," information "causing hate, disrupting the unity, stabilization and peace," "sexually explicit material that is culturally in appropriate" and statements "against any existing law."

The Draft Law does not provide guidance on how to interpret the phases used – particularly "misinformation" and references to "unity, stabilisation and peace" – noting that "statements against any existing law" effectively limits any critique or commentary on the laws of Myanmar.

Of particular concern is the reference to an online service provider having an obligation to "prevent" such content – which potentially gives rise to an obligation on internet service providers and online platform providers to proactively monitor and manage the users and content being accessed via their service which is operationally onerous and opens businesses to additional liability.

Businesses should consider their ability to respond to such requests – particularly internet service providers and other businesses who provide "online platforms" for communication. In effect the Ministry will have a broad discretion to request businesses remove online content and such request must be actioned by businesses "in a timely manner".

3.3 Government Access to data

The Draft Law includes various provisions requiring online service providers to assist authorities in the conduct of any investigations on criminal or other matter, including provision of access to user data and information requested.

The Draft Law also provides authorities with broad set of rights to intercept online communication, for reasons such as preventing actions that can harm the sovereignty and territorial integrity of the State, for defence and security, for rule of law and public order, investigating crimes, and safeguarding public life, property and welfare.

These broadly stated and otherwise undefined reasons mean that authorities could readily undertake interceptions and surveillance of online communications. Whilst there are some privacy protections under the Law Protecting the Privacy and Security of Citizens 5/2017 which required a warrant or order issued before interceptions could be undertaken,

the stipulations of certain relevant Sections of this law have been recently suspended by the incoming military regime.

Businesses should consider the implications of these broad access rights operationally, as well as in relation to their broader compliance requirements.

3.4 Electronic Transactions

The Draft Law repeals the Electronic Transactions Law (State Peace and Development Council Law No 5/2004) and replaces it with a simple regime permitting the entering into agreements using electronic technology and setting out a framework for sending and receiving electronic notices.

Whilst the Draft Law states that electronic identification permits and digital signature providers must apply for licences under the Draft Law, it does not provide any clarity on the use and operation of esignatures and digital signatures, nor the validity of agreements entered into electronically under the previous Electronic Transactions Law.

Businesses should consider the impact of this amendment on their current use of esignatures and digital signatures, and assess potential risk of having historical agreements entered into electronically under the previous Electronic Transactions Law re-executed.

3.5 Privacy & Personal Data Holders

The Draft Law sets out a framework defining "personal data" and the regulation of its use by businesses. These provisions are broadly in line with the Law Protecting the Privacy and Security of Citizens 5/2017 (noting that the stipulations of certain relevant Sections of this law have been recently suspended by the military regime). Notably it does not cover the collection of personal data, however does specify high-level principles in relation to how data is protected and processed. Personal data is only to be used disclosed, modified, copied, or destroyed in accordance with consents obtained, however the process and details of this consent process have not been fully defined.

The Draft Law also provides for disclosure of personal data to authorities under a broad range of purposes, including investigations, provisions of evidence, detection by the government departments – effectively giving authorities broad rights of access.

Businesses receiving personal data as part of their operations should carefully consider their ability to comply with requirements under the Draft Law – particularly in relation to the consents it has in place with data subjects and whether they align with the current use of such data, and measures in place to maintain confidentiality of personal data.

3.6 Consequences of breach

Breach of the Draft Law by online service providers is punishable by a sentence not exceeding three years and a fine not exceeding 100 lakhs or both.

Businesses should also be aware of specific offences relating to creating a "fake account, website and web portal", or "misinformation and disinformation" with the intent of public panic, loss of trust or social division also attracts the same penalty, as does trading in digital currency or cryptocurrency.

Given the consequences of breaching the Draft Law can be considered excessive and includes custodial sentences, Businesses are well advised to ensure they are aware of the application of the Draft Law and are compliant.

4. Conclusion

As set out above, should the Draft Law be legislated in its current form, there is no doubt that businesses operating or seeking to operate online in Myanmar, or are otherwise involved the ICT sector in Myanmar, will be significantly impacted. The following risks stand out as the main immediate concerns for business:

– Key details regarding the operation of the Draft Law, and approval rights (including the right to operate) have been delegated to yet to be established regulatory bodies;

– Potentially onerous data localisation, storage and retention requirements may impact the operation of businesses in Myanmar;

– Authorities have broad rights to intercept communications, access data and request information of online businesses;

– Regulators have grounds to suspend or terminate online business operations, and may request online operators to remove hosted content or prevent content from being shared online;

– Limited guidance has been provided for the interpretation for key terms used in the Draft Law, leading to uncertainty in application;

– Interaction of the Draft Law with other related laws such as telecommunications law, electronic transactions law, and data privacy law, is not clear and may lead to conflicting compliance requirements; and

– Severe penalties apply for breach of the Draft Law, including fines and imprisonment for up to three years;

Contacts

Simon Makinson
Head of Myanmar Practice
Tel +852 29747283
simon.makinson@allenovery.com

Michael Reede
Partner – Sydney
Tel +612 9373 7731
michael.reede@allenovery.com

James Mythen
Partner, ASEAN – Singapore
Tel +65 6671 6077
james.mythen@allenovery.com

Matthew Hodgson
Partner – Hong Kong
Tel +852 2974 7135
matthew.hodgson@allenovery.com

Saranpaal Calais
Senior Associate – Sydney
Tel +612 9373 7588
saranpaal.calais@allenovery.com

MM
CA2102063

allenovery.com