Bangkok Post The world's window on Thailand

CORPORATE COUNSELLOR

The new Computer Crimes Act and concerns over online freedom

Published: 20/01/2017 at 04:00 AM
Newspaper section: Business

The Thai government's attempts to revamp the 2007 Computer Crimes Act (CCA) and grant authorities more power to investigate and apprehend perpetrators of increasingly diverse cybercrimes has raised consternation among internet users. Many fear the new and more stringent law may impinge on human rights and place restrictions on online activity in the country.

The National Legislative Assembly (NLA) passed draft amendments to the 2007 CCA on Dec 16, and it is now awaiting publication in the Government Gazette. The law will come into effect 120 days after its publication date.

According to a report by the NLA committee responsible for drafting the amendments, they are intended to:

♦enhance and update the 2007 CCA, which is outdated due to rapid changes in the nature of cybercrimes;

♦introduce new committees; and

♦adjust and rationalise the authority of officials under the new law.

However, the public appears not to share the government's thinking behind this rationale. Before the law was passed, more than 340,000 people signed an online petition objecting to the amendments as they believe the new CCA gives excessively broad authority to government agencies to act against online content containing information that is deemed inappropriate.

The activists fear abuse of the enhanced powers under the new law could adversely affect the rights of people both inside and outside the country. Particular attention is focused on Sections 14, 18 and 20 of the CCA.

Under the new NLA-approved Act, Section 14 introduces more offences and offers more room for interpretation. Under this section, members of the public are prohibited from entering (or knowingly sharing) a computer system that causes "damage to the public, creates panic, or causes harm to public infrastructure, national security, public security or economic security".

The broad scope of the new Section 14 operates as a catch-all for a wide range of offences, thus compelling online users -- including businesses -- to be more discreet and mindful of publicly sharing information. Some argue this will force users to be more responsible in disseminating content online, while others contend that it serves to restrict freedoms for internet users.

Section 18 has also been severely criticised, as it broadly empowers officers investigating an offence under the CCA or other laws to inquire, request, access, seize, duplicate and unlock computer systems to obtain the data in question. However, a court order is specifically required for the access, seizure, duplication or hacking (unlocking) of computer systems that are not in the possession of the officers.

Although no mechanism is prescribed under the law to detail how the courts should exercise their judicial discretion in granting or declining an order, the wording of this section appears intended to limit questions about whether officers are deliberately or excessively exercising their broad authority over computer data they do not possess.

But Section 18 does not require officers to obtain a court order if they wish to request service providers, such as online access providers or social media platforms, to provide "traffic data" information to facilitate an investigation into an offence under the CCA or other laws.

Although the public has questioned why a court order is not required, these new powers will undoubtedly cause businesses and other public users to be more mindful of handling their traffic data, which could also be interpreted to include data messages sent through work or personal devices and computers.

Section 20 requires the formation of a new Computer Data Screening Committee to be appointed by the Digital Economy Ministry, wherein three out of nine members must be representatives from the private sector, including human rights, media and other related fields.

This committee will have the authority to consider and provide second-tier approval to censor "inappropriate" computer data (defined as against good morals or public order) before the request to censor the "inappropriate" computer data can be submitted for court approval. The subsequent granting of court approval will result in such data being censored. However, the public has questioned whether authorities need this type of oversight of all inappropriate computer data.

Public attention is now focused squarely on the DE Ministry, the authority charged with ensuring the smooth implementation of the new CCA. The NLA drafting committee has recommended that the ministry conduct training and educate officials so that they have a better understanding of cybercrime investigations and computer data evidence collection, in order to ensure that enforcement of the CCA complies with their intentions.

It is hoped that correct and efficient enforcement by authorities will ease public concerns over the new Computer Crimes Act, although undoubtedly, concerns will remain as the public continues to debate whether the new act is wholly appropriate for computer and online users in Thailand. All business operators in the country will need to closely monitor the CCA's implementation and enforcement to ensure compliance.

This article was prepared by Athistha Chitranukroh, of counsel in the Corporate and Commercial group at Tilleke & Gibbins. Please send comments to Andrew Stoutley at andrew.s@tilleke.com

About the author

Writer: Tilleke & Gibbins