LAWS ON DIGITAL ECONOMY AND CYBER SECURITY

As Thailand needs laws that facilitate development of the digital economy and effectively deal with cyber security issues, the Thai Government recently approved 10 bills related to information and communication technology, cyber security, personal data protection, computer crimes and telecommunications. They are collectively called as the digital economy laws. These are:

1. National Committee for Digital Economy and Society Bill
2. Organization of Ministries, Sub-Ministries and Departments Bill
3. Electronic Transactions (Amendment) Bill
4. Computer-related Crime (Amendment) Bill
5. National Cyber Security Bill
6. Personal Data Protection Bill
7. Digital Economy Promotion Bill
8. Digital Development for Economy and Society Fund Bill
9. Act on Organization for Allocation of Radio Frequencies and Supervision of Broadcasting and Telecommunications Businesses (Amendment) Bill
10. Electronic Transaction Development Agency (Amendment) Bill.

The first bill will establish the National Committee for Digital Economy and Society to set policies and directions for the development of digital economy in Thailand. The Committee will formulate a national plan covering hard infrastructure, soft infrastructure, service infrastructure, digital economy promotion, and digital economy and knowledge.

Under the second bill, the Ministry of Information and Communication Technology will be restructured and the new Ministry of Digital Economy and Society (MDES) will be established to develop the digital economy.

The bill on amendment of the Electronic Transactions Act will amend this law for its more effective implementation. It will recognize and support cross border electronic transactions amid changes in the information and communication technologies. It will also integrate the powers and duties of the relevant agencies to support the mission of the Electronic Transactions Commission.

The bill on amendment of the Computer-related Crime Act will give the MDES more responsibility and powers to implement the law. It will also strengthen the powers of the official authorities to control, monitor and access computer data and share them with other officials.

Under the National Cyber Security Bill, the National Cyber Security Committee (NCSC) and the NCSC Office will be established. The NCSC will formulate a cyber security master plan to govern cyber threats against the national and military security, the domestic peace and order, and the national economic stability. The NCSC Office will prepare and implement approaches, measures, operation plans and projects to deal with cyber security issues consistent with the NCSC's master plan.

The Personal Data Protection Bill will govern the collection, utilization and disclosure of personal data to protect personal privacy. The draft of this law had been prepared and reviewed several years before it was approved in principle by the Government.

The last four bills will establish and fund relevant agencies and amend the functions of some existing government offices and independent organizations to improve their effectiveness, transparency and collaboration and to reduce duplication of work.
As of February 2015, these bills are being reviewed by the Council of State and they will be later returned to the Government for forwarding to the National Legislation Assembly (NLA) for enacting as laws.

Concerns have been raised that the bills as drafted will infringe the freedom of expression and the right to privacy. For instance, under Section 35 of the National Cyber Security Bill, the NCSC can access information on computers, cell phones and other electronic devices of a person without a court order. Also, the draft amendment to the Computer-related Crime Act will allow competent authorities to block a website without approval from the NCSC or a court order. The concerns raised are valid and understandable. But they would not stop the Government and the NLA from passing these laws to lay down the legal framework for Thailand to achieve a digital economy. Most, if not all, of these laws will be passed sooner rather than later. The good news is that the legislators have shown willingness to address the concerns raised. For example, it is likely that the NLA will add provisions to the Personal Data Protection Act to require authorities to obtain a court order before they can access the private data.

Passing laws to support the digital economy scheme and to govern the cyber security is a daunting task. Some of these digital economy laws were passed several years ago. But the continuing changes in the information and communication technologies make it impossible to have perfect digital economy laws. The legislative work for this kind of laws cannot be a one-time process. It is a continuing task to create effective laws relevant to the prevailing environment. The laws once enacted can always be adjusted through amendments and enactment of additional legislations.

Thailand is one of the most vulnerable locations for cyber attacks. It has been known that government and private websites have been hacked and that hackers frequently use Thailand as their base for launching local and global cyber attacks. Computer crimes and internet frauds committed in or against Thailand are also posing serious cyber security risks. The need and urgency of having laws that would effectively deal with cyber security issues and jumpstart the digital economy are real.