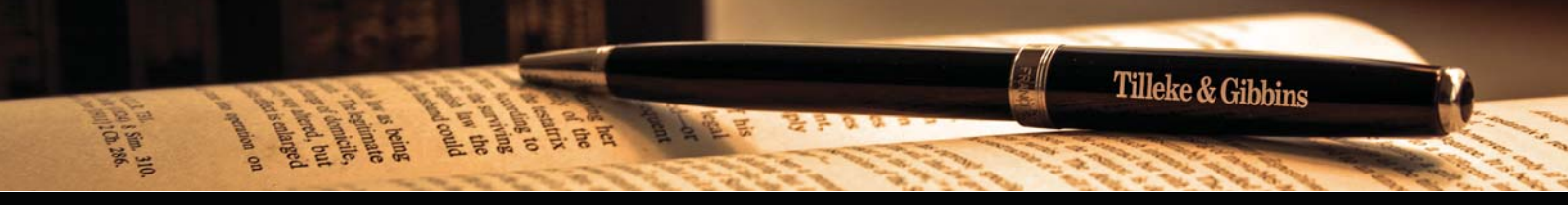
Tilleke & Gibbins
Vol. 9 No. 3 August 2018

Informed Counsel

Analysis of Recent Legal Developments in Southeast Asia



contents

Vietnam's Controversial New Cybersecurity Law Raises Questions

Left | **Giang Thi Huong Tran — Consultant**
giang.t@tilleke.com
Center | **Waewpen Piemwichai — Registered Foreign Attorney**
waewpen.p@tilleke.com
Right | **Tu Ngoc Trinh — Attorney-at-Law**
ngoctu.t@tilleke.com

Despite wide concern from inside and outside the country, and even after a request for postponement from 13 Vietnamese technology associations, Vietnam's new Law on Cybersecurity was finally adopted by the National Assembly on June 12, 2018, after more than a dozen drafts and extensive debate in the business and government sectors. The Cybersecurity Law will come into effect on January 1, 2019.

The Cybersecurity Law applies to domestic and foreign companies providing services to customers in Vietnam over telecom networks or the internet, such as social networks, search engines, online advertising, online streaming/broadcasting, e-commerce websites/marketplaces, internet-based voice/text services (OTT services), cloud services, online games, and online applications.

With its broad scope of application, the Cybersecurity Law potentially imposes tremendous obligations on both onshore and, especially, offshore companies providing online services to Vietnamese customers. For example, the new law requires that owners of websites, portals, and social networks do not provide, post, or transmit any information that is propaganda against the Vietnamese government; instigates violent disturbances, disrupts security, or disturbs public order; contains humiliating or slanderous information; or contains fabricated or untrue information (in specified contexts).

This means websites and social networks must not post or allow their users to post "anti-state," "offensive," or "inciting" content. Furthermore, service providers must develop mechanisms to monitor, verify, and take down prohibited content posted by their users within 24 hours after receiving a request from government authorities. Similar but conflicting requirements exist in other legislation; for example, regulations on general websites and social networks set a time limit of three hours for service providers to take down violating content. This is a discrepancy that will need to be resolved or have further guidance for implementation.

These requirements may diminish the website/social network operators' "safe harbor" under other valid legislation that protects them from the responsibility to monitor or supervise their users' digital information, or investigate breaches of the law arising from the process of transmitting or storing their users' digital information.

In addition, domestic and foreign companies providing services in Vietnam over telecom networks or the internet, or value-added services in cyberspace must:

- authenticate users' information upon registration;
- keep user information confidential; and
- cooperate with Vietnamese authorities to provide information on their users when such users are investigated or deemed to have breached laws on cybersecurity.

Continued on page 2

Vietnam's New Cybersecurity Law (from page 1)

Furthermore, Article 26.3 of the new law states:

> *"Domestic and foreign enterprises providing services on telecommunication networks or the internet or value-added services in cyberspace in Vietnam with activities of collecting, exploiting, analyzing, and processing personal information data, data on the relationships of service users, or data generated by service users in Vietnam must store such data in Vietnam for the period prescribed by the government."*

This language is broad and vague enough to cover a wide range of businesses and data in this current high-tech era. In addition, it is not clear how these requirements would actually be implemented in practice unless there are subordinate regulations specifically providing guidance for its implementation. For example, would a small social network of animal lovers sharing information about pets be required to open a branch or representative office in Vietnam, just because it provides social network services in cyberspace and collects personal data from Vietnamese users who join the network?

It is worth noting that some restrictions on cross-border transfer of Vietnamese users' information found in earlier drafts of the law have been removed or relaxed in the adopted version. Under the new law, both onshore and offshore online service providers appear to no longer be required to store their users' information "only" within Vietnam and comply with specified assessment procedures before transferring any "critical data" outside of Vietnam. Instead, they are simply required to store Vietnamese users' information within Vietnam for a certain period of time. However, during this statutory retention period, the law does not appear to expressly prohibit the online service providers from duplicating the data or transferring/storing such duplicated data outside of Vietnam.

Further, the controversial requirement from previous drafts that offshore service providers must place servers in Vietnam has also been removed from the final version. However, by requiring offshore service providers to "store" Vietnamese users' information in Vietnam, the law effectively forces these providers to have servers in Vietnam, either by directly owning/operating the servers or leasing servers owned/operated by other service providers in Vietnam to store such information.

Another area of concern is that the broad scope and power given to the cybersecurity authorities may create a high risk of abuse if there are no proper procedures in place and/or no further regulations on how and when they can take action on content and other issues. The law requires companies not only to comply with the cybersecurity authorities' requests and instructions, but also to help them implement their cybersecurity protection measures, which include blocking or restricting the operation of information systems (Article 5.1 and 42.3). Moreover, the cybersecurity authorities will be authorized to conduct ad hoc inspections of an organization's information systems when there are cybersecurity incidents or breaches considered critical to national security (Article 13). This could also put individual privacy at risk, with personal information subject to being scrutinized by the cybersecurity authorities.

Many industry experts have expressed concerns that the law will create obstacles and disadvantages for cyberspace activities and the business environment in Vietnam, and have questioned how the law would effectively achieve its purpose of ensuring national security. In particular, the most problematic issues of data localization/retention and business presence requirements in the law could be seen as a big step backward, which could potentially have adverse effects on international commitments made by Vietnam in multilateral trade agreements, such as the EVFTA, CPTPP, and Vietnam's WTO Commitments, all of which promote trade liberalization and minimizing technical barriers to trade.

Time will be needed for the Vietnamese government to prepare to implement the Cybersecurity Law, and many details will need to be further clarified. According to public statements from the Director General of the Cybersecurity Department of the Ministry of Public Security, 25 subordinate regulations (decrees and circulars) will soon need to be drafted and issued.

Any onshore and offshore online service providers wishing to provide services to customers in Vietnam would be well advised to assess the Cybersecurity Law and prepare themselves to comply with these requirements before they take effect on January 1, 2019.

Revamping of E-Money Regulations Under Consideration

Prompted by rapid developments in electronic currency, the government of Vietnam assigned the Ministry of Justice to work with the State Bank of Vietnam to assess the country's current legal framework for e-money management, and propose changes to the regulations. Accordingly, the State Bank released, for public consultation, a draft report on its review and proposals on June 4, 2018. A final report is to be made to the government later this year.

The State Bank studied Vietnam's existing e-money regulations as well as the management of e-money in other countries, and identified the following limitations in the current legal framework:

- Existing regulations on e-money have not kept pace with the changes in international practice. While other countries have specific regulations, or even laws, devoted to e-money, Vietnam's regulations on e-money are scattered across various pieces of legislation. A comprehensive, unified regulation is needed.
- It is necessary to clarify the nature of e-money to determine the scope and subjects of state management. In particular, there must be an official, standard definition of what e-money encompasses. The State Bank noted that "e-money," including prepaid bank cards and e-wallets, as well as money stored in mobile phone accounts, differed from "virtual currency" like bitcoin.
- Specific regulations on the management of e-money supply and issuance have some shortcomings. For example, prepaid bank cards are subject to essentially the same regulations as debit cards and credit cards, despite being different in nature; and non-bank issuers of e-money are not regulated as tightly as banks. Strict conditions must be placed on organizations supplying and issuing e-money.

The report concluded with two proposals: (1) to conduct further research with the aim of amending and supplementing Decree 101 on non-cash payment, and (2) to add "provision of payment services, not via customer's payment account" as a conditional business line under the Investment Law to have a legal basis for placing conditions on non-banking institutions issuing e-money.