COMMENTS ON THE DRAFT DECREE ON PENALTIES FOR ADMINISTRATIVE VIOLATIONS IN CYBERSECURITY

KHANH QUYNH

In order to concretize some provisions related to the penalities for administrative violations against the Cybersecurity Law as well as to systemize the regulations currently scattered in various administrative sanction documents on information technology, telecommunications, commerce, finance, banking, etc., the Draft Decree on Penalties for Administrative Violations in Cybersecurity (**Draft Decree**) is being developed by the Ministry of Public Security and undergoing public consultations by agencies, organizations and individuals. In this Legal Newsletter, NHQuang&Associates would like to analyze some regulations potentially impacting the businesses once this Decree comes into force.

Regulations on subjects to be sanctioned for administrative violations in cybersecurity

Organizations subject to sanctions are not only limited to organizations established under Vietnamese law, but also foreign enterprises, branches, representative offices, business locations of foreign enterprises providing services of telecommunications, Internet; services of content provision in cyberspace, information technology, cybersecurity, cyberinformation security; organizations and enterprises providing services of information content in cyberspace; organizations and enterprises registering domain names; information system administrators; information system operators; political, social, professional organizations and other non-business units.

Particularly, administrators of information system are authorities, organizations and individuals authorized to directly manage the information system. For State agencies and organizations, administrators of information systems are ministers, ministerial-level bodies, Governmental agencies, People's Committees of provinces and centrally-run cities or the competent authorities making decisions in investment projects for the construction, establishment, upgrade and expansion of such information systems in accordance with Clause 1, Article 3 of Decree 85/2016/ND-CP on assurance of information system security by classification.

In accordance with the above regulations, it is found that the scope of sanctioned subjects in cybersecurity is quite wide because it covers nearly all subjects from domestic and foreign individuals to organizations involved in transmitting, using and controlling information. This reveals the State's viewpoint in tightening the control over cybersecurity. Thus, organizations operating in Viet Nam, whether they are Vietnamese or foreign enterprises, may possibly be the subjects of the Draft Decree if they perform any activity in cyberspace.

Regulations on acts of administrative violations in cybersecurity

The violation acts are specified in 35 articles and classified into 5 large groups including (1) Violation of regulations on ensuring information security, (2) Violation of regulations on protection of personal data, (3) Violation of regulations on cyber-attack prevention, (4) Violation of regulations on implementing cybersecurity protection activities, (5) Violation of regulations on preventing the behaviors of using cyberspace, information technology, electronic means to violate the laws on social order and safety.

For each administrative violation in cybersecurity, an organization may be subject to warning or pecuniary sanction from 40 million to 200 million Viet Nam Dong, depending on the behavior and severity of the violation. Particularly, based on the nature, extent and consequences of the violation, the violators and aggravating circumstances, the number of violating times, the highest pecuniary sanction level may be up to 5 times of the prescribed fine or even 5% of the total revenue of the enterprise in Vietnamese market. Together with such key penalties, the Draft Decree also determines additional penalties such as depriving licenses, certificates, practice certificates or suspending operations for a definite term, etc. Simutaneously, additional remedial measures are applied, such as forced removal of the relevant programs and software; forced recall or destruction of the related products and equipment, stop of providing services harmful to cybersecurity; rectification of information violating the cybersecurity law, etc.

With the provisions in the Draft Decree, the behaviors to be sanctioned for administrative violations in cybersecurity have been specified and consistently applied. Specially, the violations addressed in the Cybersecurity Law and a number of guiding documents, but without sanctions, are now providedin more details. The following are some regulations that may generate adverse impact on businesses:

- *Regulations on violations in personal data protection (from Article 14 to Article 30)*

The Draft Decree has specified the sanctions corresponding to the issues mentioned in the Draft Decree on Personal Data Protection - the first comprehensive legal framework on data protection and privacy law established in Viet Nam. Accordingly, this Draft Decree provides in details the violations related to processing, accessing, storing, deleting, destroying, protecting, buying and selling personal data, and transferring personal data across borders, etc.

Notably, the Draft Decree has also mentioned the responsibilities of the Data Controller, the subject not yet governed in the current Draft Decree on Personal Data Protection (the latest draft is posted on the Portal of the Ministry of Public Security on February 9, 2021). This may be a new point and will be updated in the forthcoming draft version of the Decree on Personal Data Protection.

As we have seen, once such regulations are approved, they shall bind and apply directly to all businesses which are storing and processing personal data. The businesses that do not comply with the regulations on personal data protection will be at a risk of apecuniary sanction of up to 200 million Viet Nam Dong or even up to 5% of their total revenue in Viet Nam for violations repeated from the third time or more, or for disclosing or losing personal data after transfering across the border, resulting in over 1,000,000 data subjects being Vietnamese citizens. Simutaneously, such businesses also face with the interference from the management agencies in being subject to preventive measures not to conduct personal data processing or being required to stop providing services, being deprived of their licenses for personal data processing, etc. However, the Draft Decree has not yet specified the preventive measures.

- *Regulations on ensuring information security (Article 37)*

Domestic and overseas providers of services on telecommunication network, internet and value-added services in cyberspace in Viet Nam that collect, analyze or process personal information, data concerning relationships of their service users or data created by their service users in Viet Nam must store such data in Viet Nam in a specific period of time as stipulated by the Government. In particular, overseas enterprises operating in the above-mentioned fields must set up branches or representative offices in Viet Nam.

In case of violation against the regulations on data storage or establishment of branches or representative offices in Viet Nam, such organizations may be fined up to 200 million Viet Nam Dong or 5% of the total revenue in Viet Nam for any repeated violation from the third time or more; simutaneously, their right to use the business license in Vietnamese market will be deprived.

Additionally, businesses may be fined up to 160 million Viet Nam Dong if they fail to prevent or apply preventive measures not to the extent necessary to prevent information sharing or deleting within 24 hours from the time of receiving the request by competent state authorities.

Regulations on time-limit for sanctioning administrative violations

The time-limit for sanctioning administrative violations in cybersecurity is 1 year, except for cases of administrative violations related to production, trading, import, supply, exploitation and export of cybersecurity products and services. In that event, the time-limit for sanctioning administrative violations is 2 years.

Basically, the method to determine the time for calculating the sanctioning time-limit in the Draft Decree shall follow the principles of the Law on Handling Administrative Violations. Specifically, in the case that an administrative violation has ended, the time-limit is calculated from the time of termination of the violation. For ongoing administrative violations, the time-limit shall be calculated from the time when the behavior is detected.

However, the Draft Decree provides further details in some special cases. Accordingly, for violations related to financial, credit and banking activities, the time-limit is calculated from the time of termination of the violations, which is the date on which the parties fulfill their obligations; for acts of registering, notifying, performing administrative procedures; failing to submit, issue internal regulations; and issuing internal regulations not in compliance with the law, the time-limit for sanctioning shall be the date of registering, notifying, performing the administrative procedures, submitting and issuing internal regulations. This provision contributes to more consistent and clearer application of the law.

Currently, the Draft Decree is still undergoing consultation and may have other noble amendments. Enterprises should frequently update the relevant information and follow up the process of the Draft to ensure that their activies as well as policies are in compliance with provisions of laws. We shall continue with further update once the Decree officially takes effect.