



LUU TUE DANG

SOME NOTES ON THE DRAFT DECREE ON ADMINISTRATIVE SANCTIONS FOR VIOLATIONS IN CYBERSECURITY AND PERSONAL DATA PROTECTION



The Ministry of Public Security is leading the drafting of a Decree on administrative sanctions for violations in the field of cybersecurity and personal data protection (**Draft Decree**). The Draft Decree has been developed amid increasing cybersecurity risks, incidents, attacks, and personal data infringements in Viet Nam, requiring the State to establish effective prevention and response mechanisms, while also aligning with the National Strategy for Cyber Safety and Security and the Plan for implementation of the Law on Personal Data Protection and the Law on Cyber Security. This article provides highlights of the

Draft Decree that may be of interest to organizations and individuals.

Firstly, the scope of application of the Draft Decree covers both Vietnamese and foreign organizations and individuals that commit administrative violations in the fields of cybersecurity and personal data protection within the territory, internal waters, territorial sea, contiguous zone, exclusive economic zone, and continental shelf of Viet Nam, on aircraft bearing Vietnamese nationality and vessels flying the Vietnamese flag. Organizations include commercial

legal entities such as enterprises (including their dependent units) and non-commercial legal entities such as socio-political organizations, socio-professional organizations, other social organizations, and state agencies in cases where they commit administrative violations that do not fall within their assigned state management functions and duties. This indicates that, if promulgated, the Draft Decree will have a significant impact on a wide range of entities in society, from the public sector to the private sector, as well as on most organizations and individuals participating in the cyber environment.

Secondly, the Draft Decree stipulates 7 groups of violations, including violations against provisions on (i) protecting national security, ensuring social order and safety in cyberspace, (ii) preventing and combating cyber-attacks, (iii) implementing cyber security protection activities, (iv) managing cybersecurity products and services, (v) combating spam messages, spam emails, spam calls, (vi) online information, and (vii) protecting personal data. Under Clause 2, Article 1 of the Draft, for administrative violations related to cyber security or personal data protection but not specified in this Decree, the sanctioning will comply with other relevant decrees of the Government on sanctioning administrative violations in the corresponding areas of state management. Therefore, businesses, organizations and individuals need to pay attention to reviewing and complying with sanctioning regulations in other specialized documents to ensure full compliance with the law. For example, in the field of securities and securities market, Decree 156/2020/ND-CP stipulates the sanctioning against any disclosure of personal information of data subjects without their consent; in press and publication area, Decree 119/2020/ND-CP sanctions the act of disclosing private life secrets of individuals, posting or broadcasting photos of individuals without their consent.

Thirdly, among other notable points, the Draft Decree (i) strengthens the state management of violations under the existing legal framework and (ii) supplements sanctions for violations related to new technology. Specifically, the Draft increases the sanction levels for a number of violations currently specified in applicable legal documents. For example, Decree 15/2020/ND-CP currently stipulates the sanction from 10 million to 20 million Vietnamese Dong for the act of sending commercial information to a recipient's electronic address without his/her consent or when the recipient has refused. However, the sanctioning level for the same act in the Draft Decree is proposed to increase from 25 million to 50 million Vietnamese Dong. This shows that the approach by the drafting agency aims at

strengthening deterrence and tightening state management in the coming time.

In addition, the Draft also adds a number of new regulations related to technology fields that have been developing in recent times such as digital assets and artificial intelligence (AI). For example, the Draft stipulates a fine of between 10 million and 20 million Vietnamese Dong for acts of posting and disseminating information on buying, selling, exchanging, donating, collecting, leasing, lending, or illegally using digital accounts (payment accounts, bank cards, e-wallets, mobile money accounts, digital asset trading accounts), and a fine of between 20 million and 30 million Vietnamese Dong along with an additional sanction of suspension of operation from 1 month to 3 months for enterprises that set up websites, social networks or accounts, specialized pages, associations or groups on social networks and e-forums to post, disseminate and guide the implementation of the above acts. For acts of using artificial intelligence (AI) technology, Deepfake or high-tech technical measures to forge biometric data (face, voice) for illegal account authentication, the Draft proposes a fine of from 25 million to 50 million Vietnamese Dong. The term "Deepfake" is not yet specifically defined in the Draft Decree; however, it is basically understood as a concept related to AI technology and can be referred to in a number of international documents such as the EU Artificial Intelligence Ac. Accordingly, "Deepfake" is defined as AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful. It can be seen that the regulator is moving towards a more comprehensive management mechanism for the digital environment, ensuring the ability to control traditional violations and new risks arising from the rapid development of technology.

Fourthly, the Draft Decree dedicates a section to stipulate violations and corresponding sanctions in the field of personal data protection. The proposed penalty is relatively strict for a number of violations, such as (i) a fine ranging from 30 million to 50 million Vietnamese Dong for organizations that collect personal data for improper scope, specific purposes, or without the personal data subject's consent before collection as prescribed by law, (ii) a fine from 50 million to 80 million Vietnamese Dong for the act of collecting, storing and forming a personal data store from the transfer of personal data for purposes other than those consented to by the personal data subjects. In addition to the application of a fixed monetary penalties, the Draft also provides a mechanism for determining the fine level based on

the revenue derived from the violation. For example, for unlawful purchase or sale of personal data, the fine can be determined from 2 times to 10 times the revenue obtained from the violation. Such revenue covers the entire value in kind, of money, valuable papers, properties, or other material benefits that an organization or individual gains, directly or indirectly, from the commission of the violation. In addition, some violations are subject to a fine based on a percentage over *the total revenue of the preceding fiscal year of the violating organization.* For example, violations against regulations on cross-border personal data transfer may be subject to a fine ranging from 1% to 5% of total revenue, of which a fine of 3% to 5% may be imposed in cases involving the leakage or loss of personal data of 1,000,000 or more data subjects who are Vietnamese citizens, or where personal data is still transferred abroad after the competent personal data protection authority has issued a decision requiring the suspension of such transfer, resulting in harm to national defense or national security. The proposal of substantial penalties and various methods of determining fines helps to improve the effectiveness of deterrence, reduce the situation of deliberately accepting fines and continue their violations because the benefits obtained exceed the penalties imposed. However, this also poses a major challenge for individuals, organizations and businesses in strengthening compliance to avoid legal risks, remediation costs and adverse impacts on business operations.

The development of the Draft Decree on administrative sanctions for violations in the field of cybersecurity and personal data protection is necessary to improve the efficiency of state management, ensure a safe and transparent digital environment, serve economic development, and protect the lawful rights and interests of personal data subjects. The Draft has finished the consultation stage and is in the process of appraisal. Given its broad regulatory scope and extensive sanctions regime, organizations and individuals need to actively monitor updated versions, study relevant regulations, and implement appropriate compliance measures to mitigate the risk of violations when the Decree officially takes effect. In the case that our valued Clients, individuals, organizations, and businesses are interested in or have any questions related to the Draft Decree or other issues related to the field of cyber security and personal data protection, NHQuang is ready to provide appropriate legal answers and opinions.

Disclaimer:

This article is provided for general informational purposes only and is not intended to provide legal advice with respect to any specific case.

The legal provisions referred herein were effective at the time of publication, but may no longer be in effect at the time you access this article.

Please visit us at:

