

Vietnam's data regulations: Balancing national security and external pressures

By Thi Hang Banh and Thi Hong Hanh Phan

AMID increasing restrictions in Europe and the United States, TikTok, the Chinese-owned video-sharing app, faced a new probe in Vietnam. In May 2023, the country's Ministry of Information and Communications announced an investigation into TikTok's compliance with its content management, data regulations and tax obligations. The comprehensive inspection reflects the country's growing concerns about data regulations and national security in the digital age.

Vietnam's digital economy has witnessed remarkable growth, contributing 14 per cent to the nation's gross domestic product in 2022. The country also experienced a surge in online activities, with over 94.2 million smartphone users and 82.2 million mobile broadband subscribers in 2022, representing over 74 per cent of the population. As Vietnam's digital economy continues to flourish, it faces the dual challenge of safeguarding national interests while adhering to international pressures and trade agreements. Vietnam's data governance framework is anchored in its 2018 Cybersecurity Law (CSL), Decree 53 of 2022, and the recently enacted Decree 13 on Personal Data Protection in 2023. The data localisation requirement appears to favour foreign firms.

While the CSL requires all companies handling Vietnamese users' personal data to store the data within Vietnam, regardless of their origin, the guiding Decree 53 imposes this requirement solely on domestic companies. Foreign firms operating in 10 specific sectors are subject to data localisation if requested by the Ministry of Public Security (MPS) due to CSL violations. This approach seems to be a strategic move to align with international trade pacts, including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP), which prohibit requiring data localisation as a precondition for doing business in a member party.

A lenient cross-border data transfer mechanism

Vietnam's approach to cross-border data transfers is comparatively more rigid than those of China or the European Union, relying on a single mechanism. However, the country adopted a more lenient cross-border data transfer mechanism to showcase its commitment to aligning with global data regulation standards. Businesses are only required to submit impact assessment reports to the MPS within 60 days of data processing commencement. The requirement for impact assessment reports, while providing a pathway for data transfers, places a significant responsibility on companies to ensure compliance. They must navigate complex legal and security considerations to show that their data transfer does not threaten national security or compromise user data protection.

Vietnam also requires firms to implement measures for personal information protection. This entails appointing a department and designated personnel responsible for handling sensitive personal data, such as health records, financial information, and location data. However, micro, small and medium-sized enterprises (MSME) and startups directly processing personal data are exempt from this requirement.

While this exemption aims to incentivise innovation and growth, it raises concerns about the potential vulnerability of personal information. Given the limited infrastructure conditions of MSMEs and startups, there is a risk that personal data processed by these companies may be more susceptible to breaches, unauthorised access or misuse. Vietnam's data governance resembles the limited model observed in China, as highlighted by a recent study from the Asia Competitiveness Institute. This framework encompasses data localisation requirements, restrictions on cross-border data transfer and conditional access conditions. Under this model, data security is closely tied to cybersecurity and national security.

Despite granting exemptions to foreign companies, the Vietnamese government retains the authority to impose certain obligations, such as data localisation and cross-border data transfer prohibitions, in case of a CSL breach. Moreover, the CSL's broad and vague definitions of prohibited activities, subject to interpretation by the relevant authority, create a climate of uncertainty. Such ambiguity can result in self-censorship among companies. To avoid the risk of violating the law and incurring severe penalties, companies may choose to err on the side of caution by limiting or avoiding certain types of content.

While prioritising national security, Vietnam's existing data regulations demonstrate a relatively liberal stance towards foreign firms. This leniency reflects the influence of external pressures exerted by trading partners and international obligations, forcing the nation to carefully balance its own interests with its global counterparts' expectations.

Notably, calls from trading partners such as Japan and Canada for Vietnam's adherence to trade agreements such as the CPTPP resulted in revisions in regulations on cross-border data transfers. Additionally, the relaxation of data rules for foreign firms, in which American tech giants have the largest stake, was seen as a response to the US's urge for fair and reciprocal trade during the Trump presidency.

As a small country, Vietnam faces a complex challenge in developing its data policy, caught between the imperatives of national security and trading partners' demands. Striking a delicate balance becomes paramount in navigating this challenge.

The writers are researchers from the Asia Competitiveness Institute (ACI), Lee Kuan Yew School of Public Policy, National University of Singapore