LEXCOMM
Solicitors & Barristers

Legal Update on the Decree detailing a number of articles of the Law on Cybersecurity

Years after the promulgation of the Law on Cybersecurity, the long-awaited decree implementing Law on Cybersecurity has finally been introduced. On 15 August 2022, the Vietnamese Government officially issued Decree 53/2022/ND-CP detailing a number of articles of the Law on Cybersecurity (**Decree 53**).

Decree 53 has undergone a comprehensive development process from initial drafting, revising, pending to official issuance. Decree 53 is comprised of 30 articles divided into 6 chapters. It is expected to play a significant role in clarifying the implementation and compliance procedures of the Law on Cybersecurity when it enters to force on 1 October 2022.

Notably, Decree 53 shreds light on some of the hotly debated requirements under the Law on Cybersecurity which are data localisation and local presence requirements. Similar to the Law on Cybersecurity, the scope of application under Decree 53 is extended to not only local entities but also foreign entities.

In this legal update, we will highlight some major points under Decree 53 that, from our point of view, service providers in cyberspace should stay alert on.

1. Data localisation and commercial presence requirement

Before the issuance of Decree 53, the requirement on data localisation and establishment of branch or representative office in Vietnam had constantly been a matter of contention, as the Law on Cybersecurity does not provide specific regulation on types of data, period of retention, type of entities that must comply with such requirement. To address this concern, Decree 53 explicitly stipulates the types of data, the retention period and the subject entities as follows:

(a) Types of data that must be retained in Vietnam:

- Data on personal information of service users in Vietnam;
- Data created by service users in Vietnam: Service account name, service usage time, credit card information, email address, registered network address (IP) last login, logout, registered phone number associated with the account or data;
- Data on the relationship of service users in Vietnam: friends, groups with which the user connects or interacts.

(b) Entities that must comply with data localisation requirements:

- Domestic enterprise:
  All Vietnamese enterprises active in businesses mentioned under Article 26.3 of the Law on Cybersecurity must retain data in Vietnam.
- Foreign enterprises:
  Foreign enterprises must (i) retain data in Vietnam and (ii) open branches or offices in Vietnam upon the trigger of the following conditions:
  - They have business activities in 10 specific sectors[1];
  - Their services are used to commit acts of violating the Law on Cybersecurity;
  - They fail to comply, do not comply fully, or prevent, obstruct, disable or invalidate the network security protection measures after the Department of Cyber Security and Hi-tech Crime Prevention (**A05**) under the Ministry of Public Security (**MPS**) has requested/notified in writing for coordination, prevention, investigation and handling.

(c) Retention period:

- The data storage period starts from the receipt of storage request to the end of the request;
- The Minimum storage period is 24 months.

(d) Order and procedure for requesting foreign enterprise to comply with requirements on data localisation and establishment of branches or representative offices in Vietnam:

- The Minister of Public Security issues a decision requesting foreign enterprises to retain data and set up a branch or representative office in Vietnam;
- A05 notifies, instruct, monitor, supervise and urge enterprises to comply with the requests to store data, set up branches or representative office in Vietnam; at the same time, notifies relevant agencies to perform state management functions according to their competence;
- Within 12 months from the Minister of Public Security's decision, the foreign enterprise shall complete data localization, establishment of branch or representative office in Vietnam.

[1] (1) Telecommunications services; (2) storing and sharing data in cyberspace; (3) providing national or international domain names to service users in Vietnam; (4) e-commerce; (5) online payment; (6) payment intermediary; (7) transport connection services through cyberspace; (8) social networks and social media; (9) online video games; (10) services of providing, managing or operating other information in cyberspace in the form of messages, voice calls, video calls, email messages, and online chats (*Article 26.3(a) of Decree 53*)

As noted above, Decree 53 has clarified that while every Vietnamese enterprise must retain data in Vietnam, foreign enterprises are only subject to requirement on data localisation and establishment of office and branch in Vietnam only if the following conditions are triggered (i) they have business activities in regulated sectors, (ii) they have services that are used to commit violations to the Law on Cybersecurity and (iii) they fail to comply, does not comply fully, or prevent, obstruct, disable or invalidate the network security protection measures undertaken by government authorities.

2. Government authorities' power

Decree 53 provides government authorities with broad powers to implement (a) takedown measures on illegal information and fake news (b) collection measures on illegal activities (c) suspension and termination measures on the operation of information systems. Specific legal basis under Decree 53 are as follows:

(a) Takedown measures on illegal information and fake news (Article 19)

- Article 19 of Decree 53 specifies the cases in which the application of measures to request the deletion of illegal or untruthful information in cyberspace includes, *inter alia*, content that infringes upon national security or propagate against the State; incite riots, disrupt security and public order.
- Depending on the case, the Director General of A05, the heads of the Ministry of Information and Communication's competent agencies, or the Ministry of Defence's specialized force for cybersecurity protection will have the power to issue the takedown order concerning illegal content.

(b) Collection measures on illegal activities (Article 20)

- Cyberspace activities that violate national security, social order and safety, or the legitimate rights and interests of institutions, groups, and people are illegal and shall be subject to the collection conducted by competent authority.
- The Director General of A05 will determine the measure to gather electronic data for the purpose of investigating and handling such activities.

(c) Suspension and termination measures on the operation of information systems (Article 21)

- The legal bases for the suspension or stoppage of information system operation or revocation of domain names are provided as follows: (i) when there are documents proving that the operation of the information system violates the laws on national security and cybersecurity; or (ii) when the information system is being used for the purpose of infringing upon national security or social order and safety.
- The Minister of Public Security will directly issue the decision to (i) suspend, temporary suspend or request the termination of operation of the information system, (ii) suspend or revoke domain names with activities in violation of the law on network security. The Director General of A05 has the responsibility to implement the decision on suspension, temporary suspension or termination request on the operation of the information system or temporary suspension, revocation of domain name.

3. Conclusion

Compared to the draft, Decree 53 provides much clearer regulations on the implementation and compliance procedures of the Law on Cybersecurity. Upon the introduction of Decree 53, especially with further clarification on data localisation requirement, the ambiguousness under the Law on Cybersecurity has been solved. Accordingly, it has been made clear that while every domestic companies must retain data in Vietnam, foreign companies are only subject to data localisation requirement and establishment of branch or office requirement upon the satisfaction of all triggering conditions, including (i) the companies have business activities in regulated sectors, (ii) the companies have services that are used to commit violations to the Law on Cybersecurity and (iii) the companies fail to comply, does not comply fully, or prevent, obstruct, disable or invalidate the network security protection measures undertaken by government authorities.

As Decree 53 will soon come into force, stakeholders shall pay special attention to the requirements under Decree 53 and be prepared for the implementation of Decree 53.

Key contacts

If you have any questions or would like to know how this might affect your business, please contact the key contacts.

Nguyen Viet Ha
Partner
Head of Technology, Media and Telecoms
Hanoi, Vietnam
+84 24 3971 0888
ha.nguyen@lexcommvn.com

Hoang Le Quan
Senior Associate

Hanoi, Vietnam
+84 24 3971 0888
quan.hoang@lexcommvn.com

Pham Luu Ha Linh
Junior Associate

Hanoi, Vietnam
+84 24 3971 0888
linh.ha@lexcommvn.com

Legal notice