The Law on Cybersecurity

On 12 June 2018, the National Assembly passed the Law on Cybersecurity, with an affirmative vote from over 86% of delegates. The law regulates activities in protecting national security and ensuring social order and safety in cyberspace. Previous regulations on the subject had been scattered throughout different pieces of legislation, such as the Law on Information Technology, Law on Cyber-Information Security, Law on Telecommunications, Law on E-Transactions and the Penal Code.

The Law on Cybersecurity applies to local and foreign agencies, organisations and individuals who provide services in cyberspace or own any information systems and are related to cybersecurity activities in Vietnam. The scope of cyberspace covers a network of IT infrastructure, and includes telecommunications networks, internet networks, computer systems, information and processing and control systems and databases.

Presently, many foreign organisations with users in Vietnam have supplied their services on a cross-border basis into Vietnam, without necessarily having set up an establishment or entity in Vietnam. While such mode of doing business is not prohibited, these organisations are required to comply with the relevant Vietnamese laws. The Law on Cybersecurity is set to be one of those laws.

This law will come into effect from 1 January 2019.

Prohibited Acts in Cyberspace

The Law on Cybersecurity stipulates that the following acts are prohibited in cyberspace.

(i) Preparing, posting and spreading information which has propaganda that oppose the State of the Socialist Republic of Vietnam, which promotes riots, security disturbances or public disturbances, which are slanderous, or which infringes upon economic management order;

(ii) Carrying out cyber-espionage and unauthorised intrusion into State secrets and personal information on cyberspace;

(iii) Using cyberspace, information technology and electronic equipment in violating the laws of security and order;

(iv) Organising, activating, colluding, inciting, bribing, cheating, manipulating or training people to oppose the State of the Socialist Republic of Vietnam;

(v) Distorting history, negating revolutionary achievements, undermining national solidarity; offending religions and engaging in racial and sexual discrimination;

(vi) Propagating false information intended to mislead people, causing harm to socio-economic activities, causing difficulties against the activities of the state authorities or persons performing public duties, and violating the rights and obligations of other individuals and organisations;

(vii) Being involved in prostitution, social evils and human trafficking; posting obscene, depraved or criminal information; destroying the fine traditions and practices of the country, or destroying social morality and public health; and

(viii) Inciting or enticing others to commit crimes.

Websites, electronic portals and social networking sites must not provide, post or transmit information on the above or other information that violates national sovereignty and security.

The law further includes other standard prohibitions, such as those against use of cyber-attacks, obstruction of computer or telecommunications networks, unauthorised intrusions and obstructions against the authorities in their task.

Some of the above provisions are not new, and overlap with some existing laws (e.g., Decree 72/2013/ND-CP on the management, provision and use of internet service and online information). However, the law introduces many new prohibitions, such as item (iv).

The new law does not set forth administrative penalties in the event an individual or organisation breaches any of the above prohibitions – instead, the law states that it will be further detailed by the Government. However, the investigation, prosecution and handling of crimes in cyberspace will still be dealt with in accordance with the Criminal Code, Criminal Procedure Code and other relevant laws.

Salient Obligations under the Law on Cybersecurity

Local and foreign organisations that either provide services in cyberspace or which own information systems in Vietnam are to be subject to the following obligations:

(i) To establish mechanisms to verify information when users register their digital accounts;

(ii) To keep users' information and accounts secret;

(iii) To provide users' information to the specialised cybersecurity protection task force of the Ministry of Public Security upon receiving written request for the same;

(iv) To delete information and prevent the sharing of information that has content prohibited by the Vietnamese Government within 24 hours upon receiving a request by the specialised cybersecurity task force of the Ministry of Public Security ("**Cybersecurity Task Force**") or the Ministry of Information and Communication, and to archive records of the information to provide to the Cybersecurity Task Force;

(v) To not provide or to stop providing services on telecommunications networks, internet, and value-added services for organisations and individuals that publish on cyberspace content which has been prohibited by the Vietnamese Government upon request by the Cybersecurity Task Force;

(vi) To store, within the territory of Vietnam, data of users using the service in Vietnam and other important data relating to national security;

(vii) To have their headquarters or representative offices in Vietnam as specified by the Government;

(viii) To comply with requirements of the competent Vietnamese authorities concerning the investigation and settlement of violation of the Law on Cybersecurity; and

(ix) To control, prevent sharing and delete the dangerous information contents on the websites and services so that it must not cause danger or violations to children and children's rights.

The governing scope of the above obligations broad so as to include foreign organisations that provide services in cyberspace which have Vietnam-based users, regardless whether they have an establishment presence in Vietnam.

Key Takeaways and Going Forward

(A) Establishment of headquarters or representative office in Vietnam

The Law on Cybersecurity does not explicitly specify which foreign organisations providing services in cyberspace or owning information systems in Vietnam must establish their headquarters or representative office in Vietnam. As indicated in the law, this obligation is subject to further guidance by the Government.

As the law just recently approved, it remains to be seen how such requirement will be implemented – for example, whether the Government will provide a blanket requirement for all foreign organisations to have such establishment, or whether the requirement will only apply to certain organisations (such as those with a high volume of users, being a similar notification threshold adopted by *Circular 38/2016/TT-BTTTT* on the cross-border provision of public information).

At this preliminary stage, we take that the view that the latter approach is more likely. Presently, under *Circular 38/2016/TT-BTTTT*, foreign organisations engaged in the cross-border provision of public information are subject to notification requirements if they (i) lease facilities for the storage of digital information Vietnam or (ii) provide information that it reported to be used or accessed by at least 1 million internet users in Vietnam per month.

Therefore, affected individuals and organisations are advised to continue watching for further developments in this space from the Government, to determine whether or not they will legally be required to have such establishment in Vietnam.

(B) Storage of data in Vietnam

The Law on Cybersecurity also requires foreign organisations providing services in cyberspace or owning information systems in Vietnam to store data in Vietnam. The scope of data that needs to be stored comprises personal information of users in Vietnam and other relevant data that can affect national security.

However, the precise scope of data to be stored, the organisations subject to the storage requirement, and the duration in which the data is to be stored, is subject to further guidance by the Government as well. As at Section A, at this stage, we view it may not necessarily be the case that all organisations engaged in services in cyberspace will be required to comply with this data storage requirement.

(C) Requirement to Disclose and Comply with Authorities' Requirements

Note that unlike (A) and (B) above, whose scope is subject to further Government guidance, all organisations providing services in cyberspace or which own information systems in Vietnam have an obligation under the new law to supply user information upon receipt of written request by the Cybersecurity Task Force.

Furthermore, all such organisations need to generally "*comply with the requirements*" of the authorities in connection with investigations and settling of violations of the Law on Cybersecurity. The law does not specify the extent of such requirements, and appears to have been introduced as a "catch-all" provision to procure necessary cooperation from organisations

Conclusion

At present, like many of Vietnam's laws, the Law on Cybersecurity is a "framework" law, specifying obligations and requirements in general terms. It is expected that the Government or other competent authorities (e.g., Ministry of Public Security or Ministry of Information and Communications) will pass further legal instruments to guide and implement the law.

Such instruments may come out sometime between now and 1 January 2019 when the law comes into effect, so affected individuals and organisations should continue to watch out for ongoing developments in this space.

Contacts

Chau Huy Quang
Managing Partner

D +84 28 3821 2382
F +84 28 3520 8206
quang.chau@rajahtannlct.com

Vu Thi Que
Partner

D +84 28 3821 2382
F +84 28 3520 8206
que.vu@rajahtannlct.com

Logan Leung
Foreign Counsel

D +84 28 3821 2673
F +84 28 3821 2685
logan.leung@rajahtannlct.com

Cao Dang Duy
Senior Associate

D +84 24 3267 6127
F +84 24 3267 61268
duy.cao@rajahtannlct.com

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
T +65 6535 3600
F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*

Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*

Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*

Rajah & Tann (Laos) Sole Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*

Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
T +95 9 7304 0763 / +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 894 0377 to 79 / +632 894 4931 to 32 / +632 552 1977
F +632 552 1978
www.cagatlaw.com

RAJAH & TANN | *Thailand*

R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

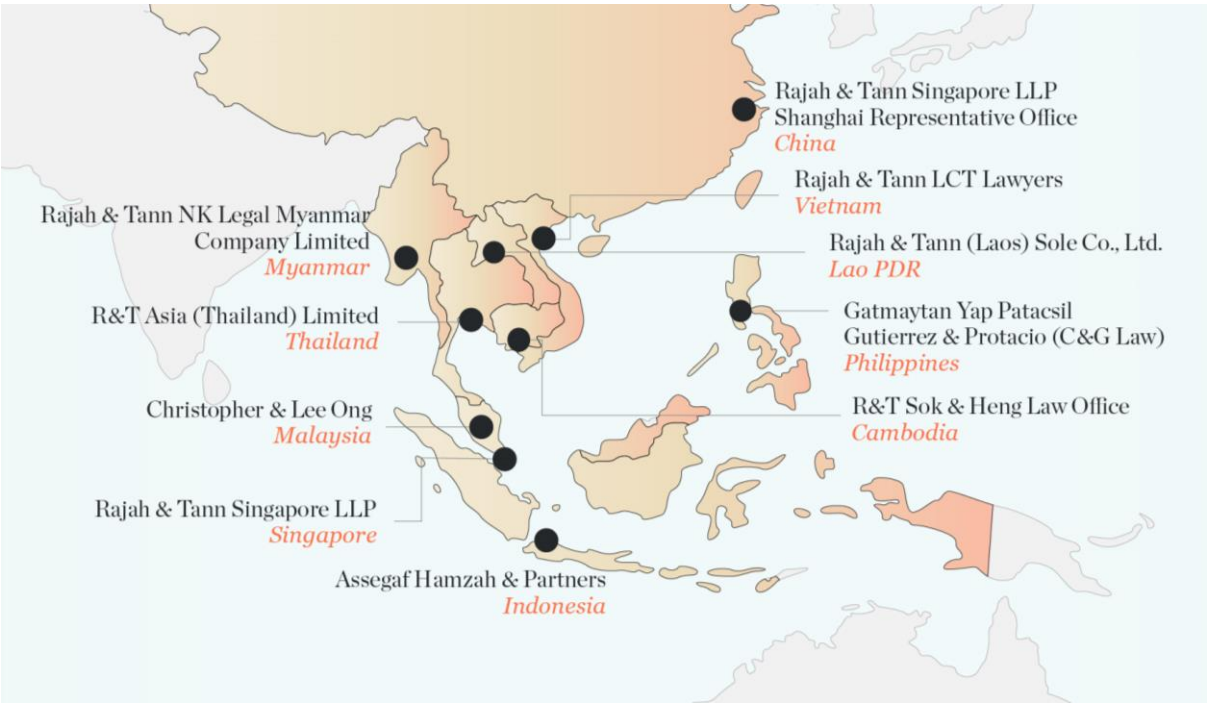
RAJAH & TANN LCT LAWYERS | *Vietnam*

Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann LCT Lawyers has a multi-faceted talent pool of lawyers with expertise in a range of practice areas who are able to provide end-to-end legal services for all transactions in Vietnam. Rajah & Tann LCT Lawyers is also able to handle cross-border transactions involving other jurisdictions, particularly those within the Indochina region.

Rajah & Tann LCT Lawyers is part of Rajah & Tann Asia, a network of local law firms in Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.