

Vietnam's New Law on Cybersecurity 2025: What's New and What Businesses Need to Know

Legal Update | December 2025



On 10 December 2025, the National Assembly of Vietnam passed the Law on Cybersecurity 2025 (**Law on Cybersecurity 2025**), which will come into force on 1 July 2026.

The Law on Cybersecurity 2025 consolidates two cornerstone statutes, Law No. 86/2015/QH13, entitled the Law on Cyber-Information Security, passed by the National Assembly of Vietnam on 19 November 2015, as amended from time to time (**Law on Cyberinformation Security 2015**) and Law No. 24/2018/QH14, entitled the Law on Cybersecurity, passed by the National Assembly of Vietnam on 12 June 2018 (**Law on Cybersecurity 2018**), into a single, unified legal framework.

Notably, according to the Law on Cybersecurity 2025, the term “cyber-information security”, which has been used under various existing legal instruments, is removed and replaced with the unified concept of “cybersecurity”. As cyber-information security has always constituted a component of cybersecurity, there remain material similarities and practical overlaps between the two concepts.

By streamlining overlapping provisions and more clearly delineating the powers of state management authorities, the Government of Vietnam aims to equip Vietnam with a more coherent and robust regulatory regime to safeguard national security, critical information systems, digital infrastructure and personal data against a backdrop of rapidly escalating cyber-attacks, data leaks, and online crime.

Although the official text of the Law on Cybersecurity 2025 is still being finalised, we highlight below the key changes introduced under the Law on Cybersecurity 2025 based on its latest draft version submitted to the National Assembly.

1. Expanded Government Oversight

Under the Law on Cyber-Information Security 2015, the Ministry of Information and Communications (**MIC**) was responsible to the Government for state management of cyber-information security, while under the Law on Cybersecurity 2018, the Ministry of Public Security (**MPS**) was responsible to the Government for state management of cybersecurity. This regulatory approach resulted in overlapping mandates and enforcement responsibilities. To address this issue, the Law on Cybersecurity 2025 consolidates state management authority by reaffirming that the Government uniformly manages state affairs relating to cybersecurity and designates the MPS as the central authority assisting the Government in this regard. The MPS is also responsible for drafting national cybersecurity standards and technical regulations. While there are measures intended to guide and improve the regulatory environment, they may present practical compliance challenges for businesses. By clearly designating the MPS as the central authority, the Law on Cybersecurity 2025 aims to streamline regulatory oversight and provide a single point of guidance for enterprises navigating these requirements.

2. Stronger Safeguards for National Security and Vulnerable Groups

The Law on Cybersecurity 2025 strengthens the protection regime for information systems, particularly systems critical to national security. While many underlying obligations are not entirely new, Articles 10 and 11 consolidate them and introduce clearer obligations on security-level classification, mandatory risk assessment and management, continuous cybersecurity monitoring, incident response and reporting. Notably, operators of information systems classified as critical to national security are subject to requirements such as mandatory cybersecurity assessment, reporting and continuous coordination with specialised cybersecurity taskforces. This enhanced framework reflects stronger controls and tighter oversight of systems considered essential to national security.

Apart from the existing safeguards for children in cyberspace that remain relevant under the Law on Cybersecurity 2025, information system administrators, businesses providing services on telecommunications networks, the Internet, and

value-added services in cyberspace are now also required to develop and implement technical systems to support activities aimed at preventing child abuse content online. Additionally, the Law on Cybersecurity 2025 also stipulates that children, the elderly, and persons with cognitive difficulties are priority target groups for cybersecurity education to enhance their ability to protect their legitimate rights and interests in cyberspace.

3. Prohibited Content and Conduct

Cyberattacks and criminal activities within cyberspace are becoming increasingly complex, causing significant damage to organisations and individuals and seriously affecting public order and national security. To address this, the Law on Cybersecurity 2025 specifies prohibited content and conduct relating to cybersecurity. In particular, in addition to inheriting regulations from the Law on Cybersecurity 2018, the provision strictly prohibits the act of (a) intentionally eavesdropping, recording, or illegally filming conversations on the internet; (b) illegally collecting, using, disseminating, exchanging, transferring, or trading personal information and data of individuals; (c) using new technologies to conduct prohibited activities.

It is also noteworthy that the scope of prohibited content in the Law on Cybersecurity 2025 is wider compared to its preceding legislation, covering, among others, (a) the inaccurate and incomplete representation of national borders, maps of Vietnam, and Vietnam's territorial sovereignty; (b) causing conflict and division among the people; (c) inciting ethnic separatism; (d) hindering the policy of international solidarity; (e) calling for boycotts of goods and services that harm businesses; and (f) impersonating information and counterfeiting the products of businesses.

4. Classification of information and information systems

The Law on Cybersecurity 2025 adopts the approach of the Law on Cyber-Information Security 2015 and maintains a five-level classification of information systems based on the extent of damage to national security, social order and safety, lawful rights and interests of individuals and organisations, and public interests in the event of incidents or violations of cybersecurity regulations. In particular, information systems are classified as follows:

- (i) Level 1: may harm the lawful rights and interests of organisations and individuals;
- (ii) Level 2: may seriously harm the lawful rights and interests of organisations and individuals, or public interests;
- (iii) Level 3: may cause especially serious harm to lawful rights and interests of organisations and individuals; serious harm to public interests; harm or serious harm to social order and safety; or harm to national security;
- (iv) Level 4: may cause especially serious harm to public interests, social order and safety, or serious harm to national security;
- (v) Level 5: may cause especially serious harm to national security.

Information systems that have been classified according to the provisions of the Law on Cyber-Information Security 2015 shall continue to be recognised. However, within 12 months from the effective date of the Law on Cybersecurity 2025, the applicable conditions, standards, and protective measures must be updated in accordance with the new classification. In cases where the level of the information system needs to be adjusted, this provision shall be applied accordingly. The Government will further detail the criteria and procedures for determining the level

of information systems and corresponding cybersecurity measures, responsibilities, and obligations for each level.

5. Compliance with Enforcement Requests

The Law on Cybersecurity 2025 introduced stricter regulations with respect to compliance with authorities' requests to combat cybercrimes. Notable requirements include coordination, provision of users' information, and content removal.

(i) Coordination request:

The Law on Cybersecurity 2025 specifies that, upon requests, businesses shall coordinate with the authority by way of (a) establishing a connection system, connecting to technical transmission lines, and transmitting data; and (b) otherwise facilitating the deployment of protective solutions and measures, for the purpose of investigating and handling violations of cybersecurity regulations.

Subject to further guiding legislation, it appears that the legal provision aims to establish a more detailed intercept mechanism from a technical perspective, by allowing the cybersecurity task forces to access business systems and request the provision of certain data. Although the requested coordination is limited to the purposes of investigating and handling cybersecurity regulations, the scope for coordination is still vague and broad, signalling uncertainty during enforcement.

(ii) Provision of user information and content removal requests:

While the Law on Cybersecurity 2018 generally required companies to provide user information for the investigation and handling of cybersecurity violations, the Law on Cybersecurity 2025 now specifies specific timeline for compliance, requiring businesses to provide user information to the specialised cybersecurity taskforce of the MPS within twenty-four (24) hours of receiving a written request, email, telephone, or other confirmed forms of communication. In emergency cases threatening national security or human life, this deadline is reduced to within three (3) hours. Similarly, in addition to the existing 24-hour deadline for preventing information sharing and removing content that violates the law, the Law on Cybersecurity 2025 specifies a new obligation to uninstall non-compliant services or applications and a 6-hour deadline upon request for deleting information in emergency cases that threaten national security.

6. Regulation of Artificial Intelligence Contents

The Law on Cybersecurity 2025 addresses the risks of new technologies, by introducing specific provisions adapted to the development of Artificial Intelligence (**AI**). It explicitly prohibits the use of AI or new technologies to falsify videos, images, or voices of others in violation of the law, and to post, spread certain prohibited content.

However, given the significant impact of AI in today's digital world, specific AI regulations will be governed by a standalone law, entitled the Law on AI.¹

7. Data Localisation and Retention

Although Vietnam's Personal Data Protection Law remains a separate legal instrument, the Law on Cybersecurity 2025 is expected to complement and

¹ Please refer to our [Legal Update - Understanding Vietnam's First Law on Artificial Intelligence](#), for further details.

reinforce data protection obligations, especially in relation to cybersecurity risk management and breach prevention.

The Law on Cybersecurity 2025 retains the data localisation requirement of the Law on Cybersecurity 2018, with further guidance to be provided by the Government.

Nevertheless, the Law on Cybersecurity 2025 further specifies the types of data that must be stored in Vietnam, such as account names, service usage time, service fee payment information, access IP addresses, and other related data.

This provision clarifies that certain data must be retained for the period prescribed by law including after the user has finished using the service.

8. IP Address Identification

The Law on Cybersecurity 2025 now requires enterprises providing services in cyberspace to identify the IP addresses of organisations and individuals using their services. This information must be provided to specialised cybersecurity forces to assist in cybersecurity management and enforcement. The Government expects that the provision would aid the investigation of increasing online crimes and fraud, gambling, or drug dealing.

Since this regulation introduces stricter requirements for the management of user information applicable to service providers, they may increase compliance costs.

9. Consolidated Framework on Cybersecurity Products and Services

The Law on Cybersecurity 2025 consolidates the existing frameworks under the Law on Cyberinformation Security 2015 with respect to cyberinformation security and civil cryptography products. The consolidated framework is called "cybersecurity products and services".

In this context, the Law on Cybersecurity 2025 stipulates the general licensing requirements for businesses providing cybersecurity products or services, which will be further elaborated by the Government.

Overall, these provisions aim to streamline administrative procedures and enhance the business environment for cybersecurity products and services.

10. Implementation Timeline and Next Steps

Although the Law on Cybersecurity 2025 has been formally passed, subordinate legislation is expected to provide further clarity on detailed compliance obligations, technical standards, and enforcement procedures.

In anticipation of the Law on Cybersecurity 2025 coming into force, organisations operating in or targeting Vietnam should consider:

- Reviewing existing cybersecurity, data protection, and incident response policies;
- Assessing whether their information systems may fall within regulated or critical categories;
- Strengthening internal governance, technical safeguards, and employee training; and
- Monitoring forthcoming implementing regulations to ensure timely compliance.

Authors



Duong Thi Mai Huong
Partner
huong.duong@frasersvn.com



Bui Tho Kien
Associate
kien.bui@frasersvn.com



Nguyen Van Long
Associate
long.nguyen@frasersvn.com

Ho Chi Minh City

19th Floor, Deutsches Haus
33 Le Duan Boulevard
Sai Gon Ward
Ho Chi Minh City, Vietnam
T: +84 28 3824 2733

Hanoi

15th Floor, Pacific Place
83B Ly Thuong Kiet Street
Cua Nam Ward
Hanoi, Vietnam
T: +84 24 3946 1203

Website www.frasersvn.com
Email legalenquiries@frasersvn.com

This material provides only a summary of the subject matter covered, without the assumption of a duty of care by Frasers Law Company. The summary is not intended to be nor should be relied on as a substitute for legal or other professional advice.