

LEGAL UPDATE

THE 2025 LAW ON ARTIFICIAL INTELLIGENCE: FROM ENABLING INNOVATION TO RISK-BASED GOVERNANCE AND LEGAL LIABILITY

1. Introduction

As artificial intelligence (AI) is increasingly deployed and exerts a profound impact across virtually all areas of economic and social life, the need for a comprehensive legal framework that both promotes innovation and ensures safety, fairness and equal protection in AI activities has become pressing. In response, the National Assembly adopted the Law on Artificial Intelligence No. 134/2025/QH15 (AI Law) on 10 December 2025, which will take effect from **1 March 2026**.¹

Building on earlier AI-related provisions in the Law on Digital Technology Industry No. 71/2025/QH15, the AI Law is Vietnam's first comprehensive legislation governing AI activities. It introduces a risk-based regulatory framework, establishes core principles, and sets out liability for damage arising from AI activities.

This legal update summarises the key regulatory pillars of the AI Law and highlights its practical implications for organisations and individuals involved in the provision, deployment, or use of AI systems in Vietnam.

2. Scope, Core Principles and Policy Objectives

The AI Law pursues a dual objective: promoting AI development as a driver of economic growth, while establishing governance mechanisms to mitigate risks and safeguard human rights and the public interest. These objectives are reflected in its scope of application, core principles, and policy orientation.

i. Scope of Regulation and Applicability

The AI Law governs the research, development, provision, deployment, and use of AI systems, together with the rights and obligations of relevant organisations and individuals, as well as the state management of AI activities in Vietnam.² AI

activities exclusively serving national defence, security and cryptography purposes fall outside its scope.³

The AI Law applies to Vietnamese agencies, organisations and individuals, and also extends to foreign organisations and individuals participating in AI activities in Vietnam,⁴ thereby capturing AI-related activities involving foreign actors conducted in Vietnam.

ii. Core Principles

A core principle of the AI Law is that AI must be "human-centred". AI activities must respect human rights, privacy, national interests, public interests, and national security.⁵

AI systems must serve humans and must not replace human authority or responsibility. The AI Law requires meaningful human control and intervention over AI-driven decisions, together with safeguards for system safety, data security, and information confidentiality, as well as supervisory oversight.⁶

In addition, the AI Law emphasises fairness and transparency, prohibits bias and discrimination, and requires compliance with ethical standards and Vietnamese cultural values, together with accountability for decisions and consequences produced by AI systems.⁷

iii. Policy Orientation

Beyond setting governance principles, the AI Law forms part of Vietnam's broader policy agenda to accelerate technological development and national digital transformation. It prioritises AI adoption in public administration and public service delivery, while encouraging wider application across socio-economic sectors to enhance productivity and governance effectiveness.⁸

¹ Article 34 of AI Law

² Article 1.1 of AI Law

³ Article 1.2 of AI Law

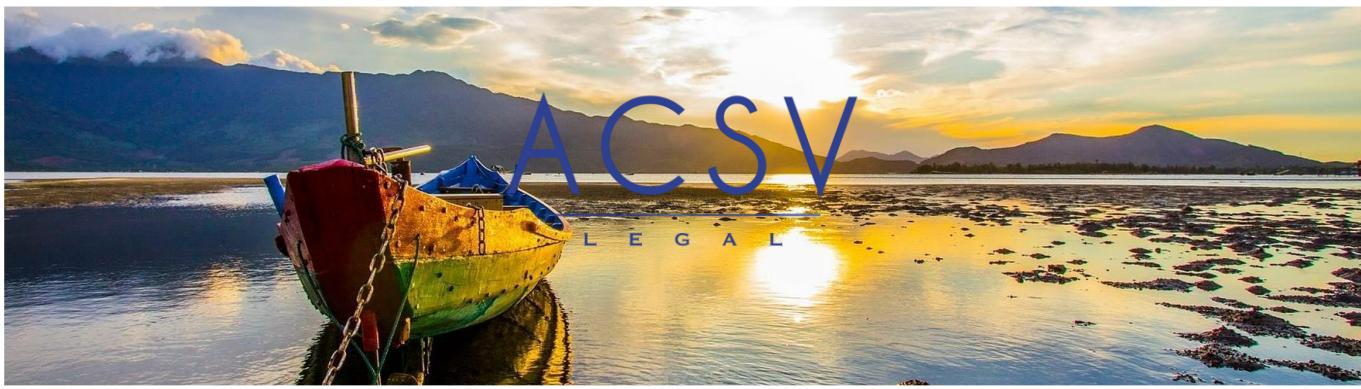
⁴ Article 2 of AI Law

⁵ Article 4.1 of AI Law

⁶ Article 4.2 of AI Law

⁷ Article 4.3 of AI Law

⁸ Article 5 of AI Law



3. Governance Mechanisms and State Management Infrastructure for AI Systems

i. Risk-Based Governance Mechanism⁹

A central feature of the AI Law is its adoption of a risk-based governance model, under which regulatory obligations and supervisory intensity are calibrated to the level of risk posed by an AI system. This approach enables enhanced control over high-risk AI systems, while avoiding undue constraints on low-risk applications.

Under the AI Law, AI systems are classified into the following three risk levels:

- **High-risk AI systems** are those capable of causing significant harm to life, health, human rights, lawful rights and interests, national interests, public interest, or national security.
- **Medium-risk AI systems** are those capable of confusing, influencing, or manipulating users because they cannot recognise that they are interacting with an AI system or with AI-generated content.
- **Low-risk AI systems** are those that do not fall within the two categories above.

The AI Law requires the provider to self-classify an AI system prior to its deployment. For medium-risk and high-risk AI systems, the provider must notify the classification results to the competent authority via the one-stop online portal on AI before the system is put into use. The deployer may rely on such classification; however, where the deployer modifies, integrates, or changes system functions in a manner that creates new risks or elevates the risk level, it must coordinate with the provider to re-classify the system.

Supervision and enforcement measures are applied on a tiered basis according to risk level, and may include inspection, monitoring, reporting obligations and other supervisory tools as prescribed by law.

ii. State Management Infrastructure

The AI Law vests unified state management of AI in the Government, with the Ministry of Science and Technology designated as the lead authority responsible for AI state management.¹⁰ It also establishes a one-stop online portal on AI to receive registrations for controlled testing,

classification notifications, serious incident reports, and periodic reports, and to publish information on AI systems and conformity assessment results.

In parallel, a National Database on AI Systems is to be developed to support regulatory oversight, monitoring, and public disclosure of information.¹¹

4. Compliance Boundaries and Innovation Support Mechanisms

i. Prohibited Acts¹²

The AI Law establishes clear prohibitions that set boundaries for the development, provision, deployment and use of AI systems. In general, AI systems must not be abused, unlawfully controlled, or exploited for illegal purposes, or used in a manner that infringes lawful rights and interests, national security, public order, or social safety.

The AI Law further prohibits AI practices that exploit vulnerabilities of vulnerable groups, manipulate or mislead users, generate or disseminate harmful or deceptive content, or undermine fairness, transparency, and ethical standards.

In addition, the collection, processing and use of data for AI development, training, testing and operation must comply with applicable laws on data protection, personal data protection, intellectual property, and cybersecurity. Any acts that obstruct or disable mechanisms for human supervision, intervention, and control over AI systems are also prohibited.

ii. Controlled Testing Mechanism¹³

To balance innovation with risk governance, the AI Law establishes a controlled testing mechanism. The results of controlled testing may be considered by competent authorities as a basis to recognise conformity assessment outcomes and to exempt, reduce, or adjust corresponding compliance obligations under the AI Law.

Competent authorities are empowered to adopt a fast-response appraisal process, closely supervise testing, and suspend or terminate controlled testing where risks arise

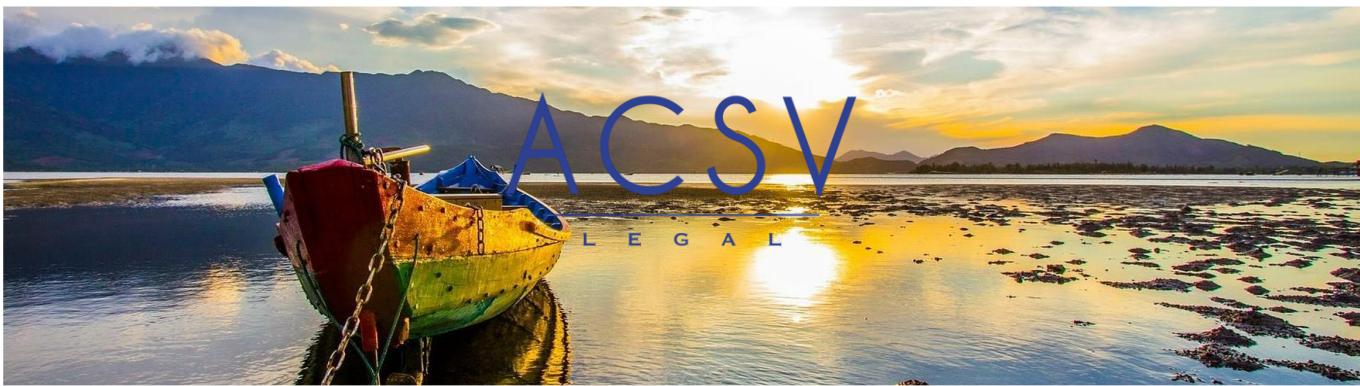
⁹ Articles 9 and 10 of AI Law

¹⁰ Article 30.2 of AI Law

¹¹ Article 8 of AI Law

¹² Article 7 of AI Law

¹³ Article 21 of AI Law



that may affect safety, security, or lawful rights and interests.

iii. National Artificial Intelligence Development Fund¹⁴

In support of AI development and innovation, the AI Law provides for establishment by the Government of the National Artificial Intelligence Development Fund, a non-budgetary state financial fund operating on a non-profit basis. The Fund may be financed by state budget allocations, contributions, grants, and donations from domestic and foreign organisations and individuals, as well as other lawful sources.

The Fund is intended to mobilise, coordinate, and allocate financial resources to promote research, development, application and management of AI in support of socio-economic development, national defence and security, and national competitiveness.

5. Legal Liability and the Compliance Roadmap

i. Liability and Compensation for AI-Related Damage¹⁵

Under the AI Law, organisations and individuals that violate AI-related requirements may be subject to administrative sanctions or criminal liability, depending on the nature and severity of the violation. Where damage occurs, civil liability and compensation are governed by Vietnam's civil law framework.

The AI Law further provides a specific compensation regime for damage caused by high-risk AI systems, including cases where such systems are managed, operated, and used in compliance with applicable requirements but nonetheless result in damage. In addition, the Law recognises liability exemptions in certain circumstances, such as where damage is caused entirely by the intentional fault of the affected party, or arises from force majeure or a state of necessity.

ii. Practical Compliance Considerations

Pending detailed governmental guidance, businesses should consider early-stage preparations, including mapping existing and planned AI systems; determining their role(s) under the AI Law; self-assessing risk levels and preparing classification dossiers (particularly for medium-risk and high-risk systems); and designing operational controls that preserve human supervision and intervention, meet

transparency obligations, and support incident management.

For AI systems already in operation before the effective date, the AI Law provides a transitional compliance timeline of 12–18 months.¹⁶ Proactive assessment and remediation during this period will help businesses minimise legal and reputational risks once the AI Law is fully implemented.

6. Conclusion

The AI Law represents a significant shift in Vietnam's governance of AI, moving from a primarily innovation-driven approach towards a combined framework of development incentives and risk-based regulation. This framework is anchored in the core principle of human-centred AI and the requirement to maintain meaningful human control and intervention over AI systems.

In practice, obligations relating to risk classification, notification via the one-stop portal on AI, transparency compliance, and the compensation regime, particularly for high-risk systems, are likely to be key focus areas for businesses.

For more information, please contact:

Nguyet Le / Special Counsel
nguyet.le@acsvlegal.com

Linh Hoang Nguyen / Associate
linhh.nguyen@acsvlegal.com

¹⁴ Article 22 of AI Law

¹⁵ Article 29 of AI Law

¹⁶ Article 35.1 of AI Law