THE NATIONAL ASSEMBLY

Law No. 134/2025/QH15

THE SOCIALIST REPUBLIC OF VIETNAM
Independence - Freedom - Happiness

LAW
ON ARTIFICIAL INTELLIGENCE

Pursuant to the Constitution of the Socialist Republic of Vietnam, which was amended and supplemented under Resolution No. 203/2025/QH15;

The National Assembly hereby promulgates the Law on Artificial Intelligence.

Chapter I
GENERAL PROVISIONS

Article 1. Scope of regulation

1. This Law prescribes the research, development, provision, deployment, and use of artificial intelligence systems (hereinafter referred to as AI-related activities); the rights and obligations of relevant organizations and individuals, and the state governance of AI-related activities in Vietnam.

2. AI-related activities exclusively for the purpose of national defense, security, and cipher do not fall within the scope of regulation hereof.

Article 2. Subjects of application

This Law applies to Vietnamese agencies, organizations, and individuals and foreign organizations and individuals involved in AI-related activities in Vietnam.

Article 3. Interpretation of terms

In this Law, the terms below are construed as follows:

1. *Artificial intelligence (AI)* means the performance of human intellectual capacities by electronic means, including learning, reasoning, perception, judgment, and natural language understanding.

2. *Artificial intelligence system (AI system)* means a machine-based system designed to perform AI capabilities with varying levels of autonomy, that may exhibit adaptiveness after deployment; and that, for explicit or implicit objectives, infers from the input data to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

3. *Developer* means an organization or individual that designs, builds, trains, tests, or fine-tunes all or part of an AI model, algorithm, or system and has direct control over technical methods, training data, or model parameters.

4. *Provider* means an organization or individual that places an AI system on the market or puts it into service under its own name, trademark, or brand, irrespective of whether the system was developed by them or by a third party.

5. *Deployer* means an organization or individual using an AI system under its authority in the course of professional or commercial activities or service provision; excluding cases of use for personal, non-commercial purposes.

6. *User* means an organization or individual that directly interacts with an AI system or uses the outputs of such system.

7. *Affected person* means an organization or individual directly or indirectly impacted regarding their rights, legitimate interests, life, health, property, reputation, or opportunities to access services due to the deployment or outputs of an AI system.

8. *Serious incident* means an event occurring in the operation of an AI system that causes or is likely to cause significant damage to life, health, human rights, property, cybersecurity, public order, environment, or disrupts the operation of critical information systems related to national security.

Article 4. Fundamental principles of AI-related activities

1. Placing humans at the center; ensuring human rights, privacy rights, national interests, public interests, and national security; complying with the Constitution and the law regulations.

2. Ensuring that AI serves humans and does not replace human authority and responsibility. Ensuring the maintenance of human control and intervention capabilities regarding all decisions and behaviors of AI systems; system safety, data security, and information confidentiality; and the ability to audit and supervise the process of development and operation of AI systems.

3. Ensuring fairness, transparency, non-bias, non-discrimination, and causing no harm to humans or society; complying with ethical standards and Vietnamese cultural values; performing accountability for decisions and consequences of AI systems.

4. Promoting the development of green, inclusive, and sustainable AI; encouraging the development and application of AI technologies towards efficient energy use, resource saving, and reduction of negative environmental impacts.

Article 5. State policies on AI-related activities

1. To adopt policies for developing AI to become a key driver for growth, innovation, and sustainable development of the country.

2. To encourage controlled technology testing (regulatory sandboxes); apply management measures commensurate with the level of risk and encourage voluntary compliance mechanisms.

3. To adopt policies ensuring rights and creating conditions for access, learning, and benefiting from AI for organizations and individuals; encourage AI development and application for the purpose of social security, supporting persons with disabilities, the poor, and ethnic minorities to bridge the digital divide; preserving and promoting national cultural identity.

4. To prioritize investment and mobilization of social resources to develop data infrastructure, computing infrastructure, safe AI, high-quality workforce, and shared AI platforms of national strategic importance.

5. To prioritize AI application in management, administration, public service provision, and decision-making support of State regulatory authorities to improve efficiency, transparency, and service quality for citizens and businesses; encourage widespread application in socio-economic sectors to improve productivity, service quality, and management efficiency.

6. To encourage organizations, networks, and social initiatives to promote safety, ethics, trust, and build social confidence in AI development.

7. To promote AI application in enterprise operations and key socio-economic sectors; develop the startup and innovation ecosystem; encourage public-private partnerships.

8. To proactively integrate and cooperate internationally; participate in building and shaping global standards and governance frameworks; ensure national interests and sovereignty in the AI field.

Article 6. Application of AI in sectors and industries

1. The application of AI in sectors and industries must comply with risk management principles in accordance with this Law and relevant law regulations.

2. For essential sectors having direct impacts on human life, health, rights and legitimate interests, or social order and safety, AI application must be managed with stricter risk levels suitable to the specific characteristics of each sector, including the following:

a) Healthcare sector: ensuring patient safety; reliability in real-world use conditions; protection of health data as prescribed by the law regulations;

b) Education sector: ensuring suitability with the age and development of learners; preventing risks in assessment, classification, and impact on learners; ensuring data safety and privacy.

3. The application of AI in scientific research activities must ensure compliance with research ethics, scientific integrity, and prevention of fraud and plagiarism during research and result publication.

4. The Government, Ministries, and ministerial-level agencies, within their competence, shall detail requirements on safety, risk management, and deployment conditions for AI application in sectors under their management, ensuring consistency with this Law.

Article 7. Prohibited acts

1. Exploiting or appropriating AI systems to commit violations of the law regulations, infringing upon the rights and legitimate interests of organizations and individuals.

2. Developing, providing, deploying, or using AI systems for the following purposes:

a) Performing acts prohibited by the law regulations;

b) Using elements of forgery or simulation of real persons or events to deceive or manipulate human perception and behavior in a purposeful and systematic manner, causing serious harm to the rights and legitimate interests of humans;

c) Exploiting vulnerabilities of vulnerable groups, including children, the elderly, persons with disabilities, ethnic minorities, or persons with loss or restriction of civil act capacity, or persons with difficulties in cognition or behavior control, to cause harm to themselves or others;

d) Creating or disseminating fake content capable of causing serious danger to national security, social order, and safety.

3. Collecting, processing, or using data to develop, train, test, or operate AI systems contrary to the law regulations on data, personal data protection, intellectual property, and cybersecurity.

4. Obstructing, disabling, or falsifying mechanisms for human supervision, intervention, and control of AI systems as prescribed in this Law.

5. Concealing information required to be public, transparent, or accountable; erasing or falsifying mandatory information, labels, or warnings in AI-related activities.

6. Abusing research, testing, evaluation, or verification activities of AI systems to commit acts contrary to the law regulations.

Article 8. AI Single-window Portal and National Database on AI Systems

1. The AI Single-window Portal is a digital platform established to support the reception and registration for participation in regulatory sandboxes; reception of notifications on AI system classification results, serious incident reports, and periodic reports; publication of information on AI systems, conformity assessment results, violation handling results as prescribed by the law regulations, and connection of support programs, funds, infrastructure, and shared data.

2. The National Database on AI Systems is built and managed centrally to serve the management, supervision, and publication of information on AI systems as prescribed by the law regulations.

3. The publication, connection, and sharing of data on the AI Single-window Portal and the National Database on AI Systems must ensure information safety and security; protection of state secrets, trade secrets, and personal data.

4. The Government shall detail the mechanism for operation, management, and exploitation of the AI Single-window Portal and the National Database on AI Systems.

Chapter II
RISK-BASED CLASSIFICATION AND MANAGEMENT OF AI SYSTEMS

Article 9. Classification of risk levels of AI systems

1. AI systems are classified according to the following risk levels:

a) High-risk AI systems are systems capable of causing significant damage to the life, health, rights and legitimate interests of organizations and individuals, national interests, public interests, or national security;

b) Medium-risk AI systems are systems capable of causing confusion, influencing, or manipulating users because they do not recognize that the interacting subject is an AI system or the content is generated by the system;

c) Low-risk AI systems are systems not falling into the cases prescribed at Point a and Point b of this Clause.

2. The risk classification of AI systems is determined based on criteria regarding the level of impact on human rights, safety, and security; the sector of use, particularly essential sectors or those directly related to public interests; the scope of users and the scale of impact.

3. The Government shall detail this Article.

Article 10. Classification and notification of AI systems

1. Providers shall self-classify AI systems before putting them into service. Systems classified as medium-risk or high-risk must have supporting classification dossiers.

2. Deployers may inherit the classification results from providers and are responsible for ensuring the safety and integrity of the system during use; in cases of modification, integration, or change of functions that give rise to new risks or higher risks, they shall coordinate with providers to re-classify.

3. For systems classified as medium-risk or high-risk, providers must notify the classification results to the Ministry of Science and Technology via the AI Single-window Portal before putting them into service. Organizations and individuals developing low-risk AI systems are encouraged to publish basic information about the system to increase transparency.

4. In cases where the risk level cannot yet be determined, providers may request the Ministry of Science and Technology for guidance on classification based on technical dossiers.

5. Inspection and supervision are performed according to the risk level of the system:

a) High-risk AI systems are inspected periodically or upon signs of violation;

b) Medium-risk AI systems are supervised through reports, sample testing, or assessment by independent organizations;

c) Low-risk AI systems are monitored and inspected upon incidents, complaints, or when safety assurance is needed, without creating unnecessary obligations for organizations and individuals.

6. Based on the results of inspection and supervision prescribed in Clause 5 of this Article, upon detection of discrepancies or dishonest declaration, competent authorities shall request re-classification, supplementation of dossiers, or suspension of use, and handle violations as prescribed by the law regulations.

7. The Government shall detail the required notification, the order and procedures for notification, and technical guidelines on risk classification.

Article 11. Responsibilities for transparency

1. Providers shall ensure that AI systems interacting directly with humans are designed and operated so that users are aware they are interacting with the system, unless otherwise prescribed by the law regulations.

2. Providers shall ensure that audio, image, and video content generated by AI systems is marked in a machine-readable format as prescribed by the Government.

3. Deployers are responsible for clearly notifying when providing to the public text, audio, images, or video generated or edited by AI systems if such content is capable of causing confusion regarding the authenticity of events or persons, unless otherwise prescribed by the law regulations.

4. Deployers are responsible for ensuring that audio, images, or video generated or edited by AI systems to simulate or impersonate the appearance or voice of real persons or recreate actual events must be labelled for easy recognition to distinguish from real content.

For products that are cinematographic, artistic, or creative works, the labelling prescribed in this Clause shall be performed in an appropriate manner, ensuring no obstruction to the display, performance, or enjoyment of the work.

5. Providers and deployers are responsible for maintaining transparent information as prescribed in this Article throughout the process of providing the system, product, or content to users.

6. The Government shall detail the forms of notification and labelling.

Article 12. Responsibilities for management and handling of AI incidents

1. Developers, providers, deployers, and users of AI systems are responsible for ensuring safety, security, reliability, and timely detection and remediation of incidents capable of causing harm to humans, property, data, or social order.

2. When a serious incident occurs in an AI system, developers, providers, deployers, and users have the following responsibilities:

a) Developers and providers must urgently apply technical measures to remediate, suspend, or recall the system, and simultaneously notify competent authorities;

b) The Deployer and User have the obligation to record, timely notify the incident, and coordinate during the remediation process.

3. Competent State regulatory authorities shall receive, verify, and guide incident handling; when necessary, they have the right to request suspension, recall, or re-evaluation of the AI system.

4. Reporting and handling of incidents are performed via the AI Single-window Portal.

5. The Government shall prescribe the reporting and responsibilities of relevant agencies, organizations, and individuals suitable to the severity of the incident and the scope of impact of the AI system.

Article 13. Conformity assessment for high-risk AI systems

1. High-risk AI systems must undergo conformity assessment as prescribed in this Law before being put into service or upon significant changes during use. In cases where there are technical standards or regulations on AI systems, conformity assessment must also be performed as prescribed by the law regulations on standards and technical regulations.

2. Conformity assessment is the confirmation that the AI system meets the requirements in Article 14 of this Law and is performed as follows:

a) For high-risk AI systems on the list of AI systems requiring conformity certification before being put into service: the assessment is performed by a conformity assessment body registered or recognized as prescribed by the law regulations;

b) For other high-risk AI systems: providers shall self-assess conformity or hire a conformity assessment body registered or recognized as prescribed by the law regulations.

3. Conformity assessment results shall be required as a condition for high-risk AI systems to be permitted for use; organizations and individuals owning assessed systems are responsible for maintaining conformity and publishing information as prescribed by the Government, serving as a basis for inspection and supervision of compliance with Article 10 of this Law.

4. The Prime Minister shall prescribe the List of high-risk AI systems, including the list of AI systems requiring conformity certification before being put into service.

5. Organizations assessing conformity or verifying AI systems must ensure independence, have sufficient technical capacity as prescribed, and be subject to periodic supervision by competent State authorities.

6. The Government shall detail this Article.

Article 14. Management of high-risk AI systems

1. Providers of high-risk AI systems shall:

a) Establish and maintain risk management measures and regularly review them when the system undergoes significant changes or new risks arise;

b) Manage training, testing, and validation data ensuring quality within technical capabilities and suitability for the system's intended purpose;

c) Compile, update, and store technical documentation and operation logs at a level necessary for conformity assessment and post-deployment inspection; provide such information to competent State authorities on the principle of necessity, proportionality to the inspection purpose, and non-disclosure of trade secrets;

d) Design the system ensuring the capability for human supervision and intervention;

dd) Perform transparency obligations and incident handling as prescribed in Article 11 and Article 12 of this Law;

e) Bear the accountability to competent State authorities regarding the intended use, operating principles at a functional description level, main input data types, risk management and control measures, and necessities for the purpose of inspection and examination; provide users and affected persons with public information at a functional description level, operation methods, and risk warnings to ensure safety in use. Explanation and information provision shall not require disclosure of source code, detailed algorithms, parameter sets, or information belonging to trade secrets or technological secrets;

g) Coordinate with competent State authorities and deployers in inspection, evaluation, post-audit, and remediation of incidents related to the system.

2. Deployers of high-risk AI systems shall:

a) Operate and supervise the system according to the correct purpose, scope, and classified risk level, ensuring no new risks or higher risks arise;

b) Ensure safety, data confidentiality, and human intervention capability during use;

c) Maintain compliance with AI standards and technical regulations during system operation;

d) Perform transparency obligations and incident handling as prescribed in Article 11 and Article 12 of this Law;

dd) Bear the accountability to competent State authorities regarding system operation, risk control measures, incident handling, and necessities for the purpose of inspection and examination; provide users and affected persons with public information at a functional description level, operation methods, and risk warnings to ensure safety in use;

e) Coordinate with providers and competent State authorities in inspection, evaluation, post-audit, and incident remediation.

3. Users of high-risk AI systems are responsible for complying with operating procedures, technical instructions, and safety measures; not intervening illegally to change system features; and promptly notifying arising incidents to deployers.

4. Explanation must be suitable to the technical capabilities of the system and not disclose trade secrets as prescribed by the law regulations.

5. Providers and deployers are encouraged to participate in civil liability insurance or apply other suitable measures to guarantee the performance of obligations for timely incident remediation and compensation for damages.

6. Foreign providers having high-risk AI systems provided in Vietnam must have a legal contact point in Vietnam; in cases where the system requires mandatory conformity certification before use, they must have a commercial presence or authorized representative in Vietnam.

7. The Government shall detail this Article.

Article 15. Management of medium and low-risk AI systems

1. Medium-risk AI systems are managed as follows:

a) Providers and deployers must ensure transparency as prescribed in Article 11 of this Law;

b) Providers are responsible for explaining the intended use, operating principles at a functional description level, main input data, and risk management and safety measures of the system upon request by State authorities during inspection, examination, or upon signs of risk or incident; explanation does not require disclosure of source code, detailed algorithms, parameter sets, trade secrets, or technological secrets;

c) Deployers are responsible for explaining the operation, risk control, incident handling, and protection of rights and legitimate interests of organizations and individuals upon request by competent State authorities during inspection, examination, or incident handling;

d) Users are responsible for complying with regulations on notification and labelling of AI systems.

2. Low-risk AI systems are managed as follows:

a) Providers are responsible for explaining upon request by competent State authorities in cases of signs of law violations or impacts on rights and legitimate interests of organizations and individuals;

b) Deployers are responsible for explaining upon request by competent State authorities in cases of signs of law violations or impacts on rights and legitimate interests of organizations and individuals;

c) Users have the right to exploit and use the system for lawful purposes and are self-responsible before the law for their usage activities.

3. The State encourages organizations and individuals deploying medium and low-risk AI systems to apply technical standards on AI.

Chapter III

INFRASTRUCTURE DEVELOPMENT AND ASSURANCE OF NATIONAL AI SOVEREIGNTY

Article 16. National AI infrastructure

1. National AI infrastructure is strategic infrastructure, comprising infrastructure invested by the State, enterprises, and social organizations; developed as a unified, open, safe ecosystem capable of connection, sharing, and expansion, ensuring satisfaction of AI development and application requirements.

2. The State plays the role of directing, coordinating, and ensuring infrastructure capacity for national AI development; encourages enterprises, research institutes, universities, and social organizations to invest in, build, and share infrastructure; strengthens public-private partnerships in AI infrastructure development.

3. The State invests in, builds, and operates AI infrastructure provided as public services, for the purpose of research, development, state-level governance, and support for innovative startups, including: computing capacity and shared data; training platforms, testing and regulatory sandbox environments; foundation models, general-purpose AI models, large language models for Vietnamese and ethnic minority languages; and other infrastructure components.

4. National AI infrastructure invested by the State, enterprises, and social organizations is connected, shared, and exploited according to standards, technical regulations, and requirements on safety, security, and data protection.

5. Important AI applications in essential sectors according to the list issued by the Prime Minister must be deployed on national AI infrastructure to ensure safety, security, and controllability.

6. The Government shall detail the mechanism for coordination, sharing, incentives, and measures to promote national AI infrastructure development, suitable to each stage and requirements for ensuring national safety and security.

Article 17. AI-ready database

1. AI-ready databases are important components of national AI infrastructure, comprising the National Database, databases of Ministries, ministerial-level agencies, Governmental agencies, People's Committees at all levels, and databases of organizations and individuals, established, managed, and exploited to serve training, testing, evaluation, and development of AI applications as prescribed by the law regulations on data, personal data protection, and intellectual property.

2. The National Database on AI is invested, built, and operated by the State at the National Data Center; organized on principles of openness, safety, and control, meeting requirements on quality, connectivity, and exploitation; comprising open data, conditionally open data, and commercial data as prescribed by the law regulations.

3. AI-ready databases of Ministries, ministerial-level agencies, Governmental agencies, and People's Committees at all levels are built, updated, and connected

consistently with the National Database on AI; ensuring standards, technical regulations, data quality, and information security.

4. AI-ready databases of organizations and individuals are encouraged to be shared with State agencies and other organizations and individuals under agreed mechanisms; sharing must comply with the law regulations on data, personal data protection, and intellectual property, ensuring rights and legitimate interests of relevant parties.

5. The Prime Minister shall issue the List of datasets to be used for AI development in essential sectors, prioritizing data on culture, Vietnamese language and ethnic minority languages, administrative procedures, healthcare, education, agriculture, environment, transportation, socio-economics, and other important sectors.

6. The Government shall detail the principles of connection, mechanisms for sharing, exploitation, and data safety assurance in AI-ready databases.

Article 18. Mastering AI technology

1. The State prioritizes the development and mastery of core AI technologies; prioritizes resources for research and development of general-purpose AI models, large language models for Vietnamese and ethnic minority languages, Vietnamese knowledge processing technology, high-performance computing and training technology, hardware, and semiconductors for AI; promotes the development and application of open-source code to enhance technological autonomy, safety, and national sovereignty in the digital environment.

2. The State promotes research, development, completion, and application of domestic AI technology; supports organizations and individuals in developing models, algorithms, software, hardware, and platform technologies; encourages resource-saving solutions that are easy to deploy and suitable for Vietnamese conditions; develops national endogenous capacity and AI innovation ecosystem; strengthens public-private partnerships to master technology.

3. Organizations and individuals researching, developing, and mastering core AI technologies are entitled to specific preferential and support policies as prescribed by the law regulations.

4. The State promotes AI application for the purpose of scientific research, analysis, and simulation, technology design and testing, automation of research, development, and innovation processes to improve national scientific and technological capacity; creating conditions to form creative capacity and mastery of the entire AI technology lifecycle.

5. The Government shall detail mechanisms, criteria, and measures to promote AI technology mastery, suitable to each development stage and requirements for ensuring national safety and security.

Chapter IV

AI APPLICATION, DEVELOPMENT OF INNOVATION ECOSYSTEM AND HUMAN RESOURCES

Article 19. National Strategy on Artificial Intelligence

1. The Prime Minister shall issue the National Strategy on AI, review, evaluate, and update it periodically at least once every 03 years or upon major fluctuations in technology and markets. Ministries, ministerial-level agencies, Governmental agencies, and People's Committees at all levels are responsible for integrating the Strategy's objectives and tasks into development strategies and plans of sectors, domains, and localities and ensuring resources for implementation.

2. The National Strategy on AI is built based on orientations for developing technology, infrastructure, data, and human resources; promoting research, mastery, and application of AI in priority sectors; ensuring safety, innovation, and national sovereignty in the digital environment. The Strategy must prescribe a system of indicators, methods, and measurement mechanisms to assess the level of national AI development.

3. The State encourages the development of AI technology groups suitable to Vietnamese conditions, having potential to create added value, being environmentally friendly, easy to apply widely, and contributing to ensuring national sovereignty in the digital environment.

Article 20. Development of AI ecosystem and market

1. Organizations and individuals operating in the AI field are entitled to the highest incentives and support as prescribed by the law regulations on science and technology, investment, digital technology industry, high technology, digital transformation, and relevant laws; are created conditions to access infrastructure, data, and testing environments for research, production, and commercialization of AI products and services.

2. The State supports the development of the AI ecosystem and market, including:

a) Prioritizing the use of AI products and services as prescribed by the law regulations on bidding;

b) Developing the market for AI products and services, including technology exchange floors and platforms connecting supply and demand;

c) Ensuring fair and transparent access to computing infrastructure, data, and regulatory sandboxes;

d) Applying preferential policies on tax, investment, and finance based on principles of encouraging research, production, and commercialization of AI products and services.

3. The State encourages the development and application of new-generation AI, promoting innovation, improving governance, production, business capacity, and public service provision.

4. Organizations, individuals, enterprises, research institutions, and State agencies are encouraged to exploit, share, and reuse data in the National Database on AI for research, training, testing, and innovation, ensuring compliance with the law regulations on data, personal data protection, cybersecurity, and intellectual property.

5. Small and medium-sized enterprises (SMEs) and innovative startups in AI are prioritized for access to technical infrastructure, data, and testing environments, and are entitled to support regarding costs, training, and market connection for the development of AI products and services.

6. The Government shall detail mechanisms, conditions, and procedures for implementing measures to support the development of the AI ecosystem and market.

Article 21. Controlled testing mechanism for Artificial Intelligence (Regulatory Sandbox)

1. The regulatory sandbox mechanism for AI is implemented as prescribed by the law regulations on science, technology, and innovation and the regulations in Clauses 2, 3, and 4 of this Article.

2. Results of the regulatory sandbox serve as a basis for competent State authorities to consider:

a) Recognizing conformity assessment results as prescribed in this Law;

b) Exempting, reducing, or adjusting corresponding compliance obligations of this Law.

3. Competent State authorities shall assume the prime responsibility for, and coordinate with relevant agencies in, receiving, appraising, and processing dossiers according to fast-track appraisal and response procedures; supervising the testing process and deciding to suspend or terminate testing upon risks affecting safety, security, or rights and legitimate interests of organizations and individuals.

4. The Government shall detail this Article.

Article 22. National AI Development Fund

1. The National AI Development Fund is an off-budget state financial fund, operating not-for-profit, established by the Government to mobilize, coordinate, and allocate resources to promote research, development, application, and management of AI for socio-economic development, national defense, security, and improving national competitiveness.

2. Financial sources of the Fund include sources granted by the State budget; contributions, aid, and sponsorship from domestic and foreign organizations and individuals; and other lawful sources as prescribed by the law regulations.

3. The Fund is entitled to apply specific financial mechanisms, accepting risks in science, technology, and innovation; flexible capital allocation according to progress and implementation requirements, independent of the budget year; applying simplified order and procedures for strategic tasks or those requiring rapid deployment. The Fund is prioritized for investment, sponsorship, and support for:

a) Developing AI infrastructure;

b) Researching, developing, and mastering core AI technologies;

c) Developing AI enterprises;

d) Training, fostering, and attracting AI workforce;

dd) Other investment and support tasks to achieve AI development objectives as prescribed by the Government.

4. The Fund operates on principles of publicity, transparency, efficiency, and proper purpose; ensuring coordination and non-duplication with other state financial funds.

5. The Government shall detail the specific financial mechanism, organization, management, use, and supervision of the Fund.

Article 23. AI human resource development

1. The State develops AI human resources in a comprehensive direction, interconnected between educational levels and training qualifications, ensuring the formation of a high-quality workforce for research, development, application, and management of AI.

2. General education integrates basic content on AI, computational thinking, digital skills, and technology ethics into the compulsory curriculum; encourages experiential, research, and creative activities involving AI.

3. Vocational education and higher education institutions are encouraged to build training programs on AI, data science, and related majors; encourage cooperation with enterprises, research institutes, and international organizations in training, internship, research, and technology transfer.

4. The State implements the National Program on AI Human Resource Development, including training policies, scholarships, attracting and employing experts, developing teaching staff, scientists, and management personnel involving AI.

5. Organizations, training institutions, research institutes, and enterprises participating in AI workforce development are entitled to encouragement and incentive mechanisms as prescribed by the law regulations, and simultaneously responsible for coordinating in training, applied research, and professional practice, linking training with practical needs.

6. Higher education institutions, research institutes, and innovation centers are responsible for cooperating, sharing knowledge, and participating in national and international networks on training, research, and development of AI human resources.

7. The Ministry of Education and Training shall assume the prime responsibility for developing, and put forward the promulgation thereof to the Prime Minister, the National Program on AI workforce development, which prescribes standards, recognition of training programs, resource mobilization mechanisms, and preferential policies for participating organizations and individuals.

Article 24. Development of AI clusters

1. An AI cluster is a cooperation network between enterprises, research institutes, universities, and relevant organizations, organized to strengthen links regarding functions, AI infrastructure, and physical space to promote innovation, AI development, and improve competitiveness.

2. The State encourages the development of AI clusters according to a model combining concentrated physical space and digital link networks; forming cluster centers at hi-tech parks, concentrated digital technology zones, and innovation centers; attracting organizations and individuals to invest in building technical infrastructure for cluster-related activities, including laboratories, testing centers, verification centers, and other support facilities meeting national and international standards.

3. Organizations and individuals being members of recognized AI clusters are entitled to the following preferential policies:

a) Priority access to and use of national AI infrastructure, shared data, and testing platforms with preferential costs;

b) Support to participate in workforce training programs, trade promotion, scientific, technological, and innovation tasks in key sectors.

4. The Government shall detail the criteria, order, procedures for recognition, operation mechanism of AI clusters, and preferential policies in Clause 3 of this Article.

Article 25. Support for enterprises involving AI

1. Innovative startups and SMEs are supported with conformity assessment costs prescribed in this Law; provided free of charge with sample dossiers, self-assessment tools, training, and consulting; prioritized for support from the National AI Development Fund.

2. Innovative startups, SMEs, science and technology organizations, and research groups with feasible innovation projects are supported through support vouchers to use computing infrastructure, shared data, large language models for Vietnamese and ethnic minority languages, training platforms, testing, and technical consulting services for research, development, and deployment of AI applications.

3. Enterprises with capacity for research, development, and innovation in the AI field are prioritized to participate in tasks within national science, technology, and innovation programs, tasks for developing high technologies prioritized for investment and development, strategic technologies, and key digital technology products and services; supported to develop core technologies, foundation models, hardware, and high-performance training technologies according to national AI capacity development orientations.

4. Enterprises participating in AI testing under the regulatory sandbox mechanism are supported with technical consulting, risk assessment, safety testing, and connection with testing and verification facilities as prescribed by the law regulations.

5. Enterprises sharing data, models, tools, or research results for AI development are entitled to incentives or support as prescribed by the law regulations, ensuring compliance with the law regulations on data, personal data protection, and intellectual property.

6. The State encourages cooperation between enterprises, research institutes, universities, and innovation centers to develop AI technology, commercialize research results, and expand innovation capacity; encourages enterprises to invest long-term in AI research and development.

7. The Government shall detail mechanisms, policies, conditions, and procedures for implementing support for enterprises in the AI field.

Chapter V
ETHICS AND RESPONSIBILITIES IN AI-RELATED ACTIVITIES

Article 26. National AI Ethics Framework

1. The National AI Ethics Framework is promulgated based on the following principles:

a) Ensuring safety, reliability, and causing no harm to the life, health, honor, dignity, and spiritual life of humans;

b) Respecting human rights and citizen rights, ensuring fairness, transparency, and non-discrimination in AI development and use;

c) Promoting happiness, prosperity, and sustainable development of humans, communities, and society;

d) Encouraging innovation and social responsibility in AI research, development, and application.

2. The National AI Ethics Framework is reviewed and updated periodically or upon major changes in technology, law, and management practices.

3. The National AI Ethics Framework serves as a basis for orienting the development of standards, technical regulations, specialized guidelines, and policies encouraging safe, reliable, and responsible AI development.

4. The State encourages organizations and individuals to apply the National AI Ethics Framework during the research, development, provision, deployment, and use of AI systems to ensure transparency, fairness, safety, and respect for human rights.

5. The Minister of Science and Technology shall promulgate the National AI Ethics Framework based on the regulations in Clause 1 of this Article.

Article 27. Ethical responsibility and impact assessment in AI application in State-level governance and public service provision

1. The use of AI systems in State-level governance and public service provision must ensure publicity, transparency, and responsibility for compliance with the National AI Ethics Framework.

2. AI systems do not replace the decision-making authority and responsibility of decision-makers as prescribed by the law regulations. Decision-makers are responsible for reviewing and using results provided by AI systems.

3. Agencies operating high-risk AI systems or those having significant impacts on human rights, social justice, or public interests must prepare impact assessment reports on system use; reports include risk identification, control measures, and assurance of human supervision and intervention capabilities.

4. Agencies preparing impact assessment reports are responsible for the content, honesty, and completeness of the report; reports are published as prescribed by the law regulations, excluding contents belonging to state secrets, trade secrets, or personal data.

5. The Government shall detail the particulars, procedures, and responsibilities for impact assessment, risk management, and supervision of AI system use in State-level governance and public service provision.

Chapter VI
INSPECTION, SUPERVISION AND HANDLING OF VIOLATIONS

Article 28. Inspection and examination

1. Inspection activities involving AI are carried out in accordance with the law on inspection.

2. Agencies and organizations assigned to perform State-level governance functions on AI are responsible for examining the compliance with the law regulations of organizations and individuals in AI-related activities.

3. During inspection and examination, relevant organizations and individuals have the obligation to provide technical dossiers, trace logs, training data, and other necessary information to identify causes of violations, incidents, or delineate responsibilities; information provision must comply with the law regulations on state secret protection, data, personal data protection, and intellectual property.

4. Inspection and examination conclusions and decisions on administrative violation sanctions must be published as prescribed by the law regulations.

Article 29. Handling of violations and liability for compensation for damage

1. Organizations and individuals committing acts violating the regulations of this Law and other relevant law regulations on AI, depending on the nature, severity, and consequences of the violation, shall be sanctioned for administrative violations or examined for penal liability; if causing damage, they must compensate as prescribed by the Civil law regulations.

2. In cases where a high-risk AI system is managed, operated, and used in accordance with regulations but still causes damage, the deployer must be responsible for compensating the damaged person. After compensation, the deployer may request

the provider, developer, or relevant parties to refund the compensation amount if there is an agreement between the parties.

3. The liability for compensation for damages prescribed in Clause 2 of this Article is exempted in the following cases:

a) Damage occurs entirely due to the intentional fault of the damaged person;

b) Damage occurs in force majeure events or emergency circumstances, unless otherwise prescribed by the law regulations.

4. In cases where an AI system is intruded upon, hijacked, or illegally intervened by a third party, the third party must be responsible for compensating for damages. In cases where the deployer or provider is at fault in allowing the system to be intruded upon, hijacked, or illegally intervened, they must be jointly liable for compensating for damages as prescribed by the Civil law regulations.

5. The Government shall detail the sanctioning of administrative violations for acts of violation caused by AI systems.

Chapter VII
STATE GOVERNANCE OF ARTIFICIAL INTELLIGENCE

Article 30. AI-related state governance contents and responsibilities

1. State governance of AI covers:

a) Building, promulgating, and organizing the implementation of strategies, policies, programs, and legal normative documents on AI;

b) Promulgating and organizing the implementation of standards and technical regulations on AI;

c) Managing, coordinating, and developing national AI infrastructure;

d) Managing and supervising AI activities;

dd) Propagating and disseminating policies and laws; statistics, reporting, scientific research, and international cooperation on AI;

e) Inspecting, examining, handling violations, resolving disputes, complaints, and denunciations regarding AI.

2. Responsibilities for State-level governance of AI:

a) The Government performs unified State-level governance of AI;

b) The Ministry of Science and Technology is the focal agency, responsible before the Government for performing State-level governance of AI nationwide;

c) Ministries and ministerial-level agencies, within their functions, tasks, and powers, coordinate with the Ministry of Science and Technology in performing State-level governance of AI;

d) Provincial-level People's Committees perform State-level governance of AI locally.

Article 31. Principles of providing information and data for the purpose of State-level governance

1. Competent State authorities, organizations, and individuals assigned to perform State-level governance activities as prescribed in this Law are responsible for ensuring the confidentiality of information, data, and trade secrets provided during task performance, including technical dossiers, training data, source code, and algorithms as prescribed by the law regulations.

2. Requests for organizations and individuals to provide information and data must ensure necessity, proportionality, and suitability with the scope, purpose, and content of State-level governance activities.

3. Provided information and data must be ensured safety and security as prescribed by the law regulations.

Article 32. International cooperation

1. International cooperation in the AI field is performed as prescribed by the law regulations on science and technology, technology transfer, other relevant law regulations, and international treaties to which the Socialist Republic of Vietnam is a member.

2. The State encourages international cooperation on sharing high-performance computing infrastructure, data, human resources, scientific research, and mutual recognition of conformity assessment results as prescribed in this Law.

Chapter VIII
IMPLEMENTATION PROVISIONS

Article 33. Annulment of a number of chapters, articles, clauses, and points of the Law on Digital Technology Industry No. 71/2025/QH15

To annul Clause 9 Article 3, Clause 7 Article 4, Clause 6 Article 12, Point dd Clause 2 Article 34, and Chapter IV of the Law on Digital Technology Industry.

Article 34. Effect

This Law takes effect from March 1, 2026, unless otherwise prescribed in Article 35 of this Law.

Article 35. Transitional provisions

1. For AI systems put into operation before the effective date of this Law, providers and deployers are responsible for performing compliance obligations as prescribed in this Law within the following time limits:

a) 18 months from the effective date of this Law for AI systems in healthcare, education, and finance sectors;

b) 12 months from the effective date of this Law for AI systems not falling into the cases prescribed at Point a of this Clause.

2. Within the time limit prescribed in Clause 1 of this Article, AI systems are allowed to continue operating, unless otherwise the State regulatory authority in charge of AI determines that the system poses a risk of causing serious damage, in which case it has the right to request suspension or termination of operation.

This Law was passed on December 10, 2025, by the 15th National Assembly of the Socialist Republic of Vietnam at its 10th session.

CHAIRMAN OF THE NATIONAL ASSEMBLY

Tran Thanh Man