

# THE MODEL ARTIFICIAL INTELLIGENCE LAW

**MAIL v.3.0**

**PREPARED AS**

Expert Draft Proposal

**PREPARED BY**

AIGVERSE

JUNE 2025

*To follow the contents of updates, please scan the QR Code below. Should there be any suggestions, comments, or questions, please feel free to reach out via [modelailaw@outlook.com](mailto:modelailaw@outlook.com)*



AIGVERSE

# THE DRAFTING TEAM

## THE COORDINATOR

- **Hui ZHOU**, Deputy Director (Acting Director), Department of Cyber and Information Law, Institute of Law, Chinese Academy of Social Sciences (CASS); Standing Deputy Secretary-General of China Cyber and Information Law Society

## THE MEMBERS (In alphabetical order of surnames by pinyin)

- **Yanlin CAO**, Director and Research Fellow, Department of Medical and Health Law, Institute of Medical Information, Chinese Academy of Medical Sciences
- **Tianhao CHEN**, Associate Professor, School of Public Policy and Management, Tsinghua University; Assistant Director, Research Center for Science, Technology and Society, Tsinghua University
- **Xingsi DI**, Assistant Professor, School of Law, Guangzhou University; Research Fellow, Research Center for the Rule of Law in Science and Technology Innovation, Guangzhou University
- **Zixuan FENG**, Executive Director and Professor, Institute for Digital Rule of Law Governance, Southwest University of Political Science and Law
- **Hongyu FU**, Director, Center for AI Governance, AliResearch
- **Bo HE**, Director and Senior Engineer, Center for Internet Law, China Academy of Information and Communications Technology (CAICT)
- **Yanqing HONG**, Professor, School of Law, Beijing Institute of Technology; Director, Center for International Governance of Cyberspace, Beijing Institute of Technology

- **Naying HU**, Senior Business Executive, Artificial Intelligence Institute, China Academy of Information and Communications Technology
- **Xueyao LI**, Professor, KoGuan School of Law, Shanghai Jiao Tong University; Director, Laboratory for Law and Cognitive Intelligence, Shanghai Jiao Tong University
- **Beizheng LIN**, Judge of the Second Rank, Guangzhou Internet Court
- **Canhua LIU**, Assistant Professor, Institute of Law, Chinese Academy of Social Sciences (CASS)
- **Jinrui LIU**, Research Fellow, Institute of Rule of Law, China Law Society
- **Lan MA**, Chief Legal Counsel, Qi-Anxin Technology Group
- **Yu SU**, Professor, School of Law, People's Public Security University of China; Director, Institute of Data Law, People's Public Security University of China
- **Jun WANG**, Director of Research, Compliance Tech Research Institute, Southern Finance Omnimedia Corp. (SFC)
- **Lei WANG**, Research Fellow, Center for Law of Intelligent Technology, Beijing Institute of Technology
- **Wei WANG**, Research Fellow (By Courtesy), Center for Artificial Intelligence Law, School of Law, Guangdong University of Finance and Economics
- **Xiang WANG**, Technical Committee Member (ISO/TC 154), International Organization for Standardization (ISO)
- **Yue WANG**, Professor, School of Law, Xi'an Jiaotong University
- **Lance Fan WU**, Executive Director, Legal Global Trade Regulations, Ethics & Compliance, Government Relations, Lenovo Group
- **Jiujiu XU**, Assistant Professor, Institute of Law, Chinese Academy of Social Sciences (CASS)

- **Zhiwei YAO**, Professor, School of Law, Guangdong University of Finance and Economics; Director, Center for Artificial Intelligence Law, Guangdong University of Finance and Economics
- **Kang YUAN**, Professor, School of Law, Wuhan University; Deputy Director, Institute of Cyberspace Governance, Wuhan University
- **Song ZHANG**, Senior Engineer, Kunlun Digital Technology Co., Ltd.
- **Xin ZHANG**, Professor, School of Law, University of International Business and Economics; Director, Center for Digital Economy and Legal Innovation, University of International Business and Economics (UIBE)
- **Yan ZHANG**, Professor, School of Law, Renmin University of China (RUC)
- **Shuyu ZHAO**, Chief and Senior Engineer, Center for Internet Law, China Academy of Information and Communications Technology (CAICT)
- **Yue ZHU**, Assistant Professor, School of Law, Tongji University; Research Fellow, Shanghai Collaborative Innovation Center of AI Social Governance
- **Lingfeng ZHU**, Executive Director of Data and Privacy Protection, MeiTuan

The English version was translated and compiled by **Wei WANG**. This translation is provided solely for reference purposes; the original Chinese version shall prevail as the authoritative text, and the final interpretation shall be based on the original Chinese version.

# TABLE OF CONTENTS

<b>CHAPTER I GENERAL PROVISIONS .....</b>	<b>1</b>
Article 1 – Legislative Basis .....	1
Article 2 – Scope of Application .....	1
Article 3 – Governance Principle .....	2
Article 4 – Human-Centric Principle.....	2
Article 5 – Safety/Security Principle .....	2
Article 6 – Principle of Openness, Transparency, and Explainability .....	2
Article 7 – Principle of Accountability .....	2
Article 8 – Principle of Fairness and Equality .....	3
Article 9 – Green Principle (of Sustainability).....	3
Article 10 – Principle of Promoting Development and Innovation .....	3
Article 11 – Principle of Ethics .....	3
Article 12 – International Cooperation.....	4
Article 13 – Competent Authorities .....	4
Article 14 – Collaborative Co-Governance .....	4
Article 15 – Legality and Legitimacy .....	5
 <b>CHAPTER II SUPPORT AND PROMOTION OF ARTIFICIAL INTELLIGENCE .....</b>	 <b>6</b>

Article 16 – Development Plan for Artificial Intelligence .....	6
Article 17 – Construction of Computing Infrastructure.....	7
Article 18 – Innovation in Algorithms and Foundation Models .....	7
Article 19 – Supply of Data as a Factor of Production.....	8
Article 20 – Statutory Licensing for the Use of Copyrighted Works in Foundation Model Training .....	8
Article 21 – Fair Use of Copyrighted Works in Training Open-Source Foundation Models .....	8
Article 22 – Artificial Intelligence Pilot Zones and Authorized Legislature .....	9
Article 23 – Free Trade Zone Exemptions .....	9
Article 24 – Dynamic Assessment of Policy and Regulatory Compatibility .....	10
Article 25 – Fiscal and Procurement Support .....	10
Article 26 – Tax Credits and Incentives .....	10
Article 27 – Industrial Development and Application Innovation .....	11
Article 28 – Promoting Innovation by Small and Medium-Sized Enterprises .....	11
Article 29 – Government-Led Pilot Applications .....	11
Article 30 – Evaluation Systems .....	11
Article 31 – Talent Cultivation.....	12

## **CHAPTER III ARTIFICIAL INTELLIGENCE OVERSIGHT**

### **SYSTEM ..... 13**

Article 32 – Categorized Oversight System.....	13
Article 33 – Negative-List Oversight System .....	14
Article 34 – Licensing Conditions for the Negative List .....	14
Article 35 – Application for Licenses within the Negative List .....	15
Article 36 – Approval of Licenses within the Negative List.....	15
Article 37 – Reapplication for licenses within the Negative List .....	16
Article 38 – Public Disclosure of License .....	16

Article 39 – Complaint, Reporting, and Clarification Mechanisms .....	16
Article 40 – Other Licenses and Registries .....	17

## **CHAPTER IV OBLIGATIONS OF AI DEVELOPERS AND PROVIDERS ..... 18**

<b>Section 1: General Provisions .....</b>	<b>18</b>
Article 41 – Safety/Security Obligations.....	18
Article 42 – Obligation to Manage Security Vulnerabilities.....	19
Article 43 – Obligation to Audit .....	19
Article 44 – Obligation to Remedy and Notify .....	19
Article 45 – Obligation of Openness and Transparency .....	20
Article 46 – Obligation of Explainability .....	21
Article 47 – Obligation of Fairness .....	21
Article 48 – Risk Management.....	21
Article 49 – Obligation of AI Ethics Review .....	22
Article 50 – Obligations of State Organs in Provision and Development .....	22
Article 51 – Designated Representatives.....	23
Article 52 – Trusted Data .....	23
<b>Section 2: Obligations of Artificial Intelligence Developers .....</b>	<b>23</b>
Article 53 – Enhanced Obligations for AI Developers on the Negative List .....	23
Article 54 – Special Obligations for Developers of Foundation Models .....	23
<b>Section 3: Obligations of Artificial Intelligence Providers .....</b>	<b>24</b>
Article 55 – Registry Obligations .....	24
Article 56 – Registry Process .....	25
Article 57 – Internal Management Systems.....	25
Article 58 – Termination Mechanism .....	26
Article 59 – Permission Revocation .....	26

Article 60 – Enhanced Obligations for Negative-Listed AI Providers..... 26

Article 61 – Obligations for Platform Operators ..... 27

Article 62 – Security of Terminal Device Permissions ..... 27

**CHAPTER V COMPREHENSIVE AI GOVERNANCE MECHANISM**  
**..... 28**

Article 63 – Responsibilities of the National AI Administrative Authority ..... 28

Article 64 – AI Ethics Expert Committees ..... 29

Article 65 – Security Review System ..... 30

Article 66 – Timeframe for Preliminary Procedures ..... 30

Article 67 – Interviewing ..... 30

Article 68 – Innovative Regulation ..... 31

Article 69 – Regulatory Sandbox ..... 31

Article 70 – Internal Whistleblower Protection and Reporting Mechanism ..... 31

Article 71 – Officials Responsible for State Organs ..... 32

Article 72 – Law Enforcement ..... 32

Article 73 – Governance through Technology ..... 33

Article 74 – Countermeasures against Foreign Entities..... 33

Article 75 – Reciprocal Measures ..... 33

**CHAPTER VI LIABILITIES ..... 34**

Article 76 – General Liabilities ..... 34

Article 77 – Revocation of Negative-List Licenses ..... 35

Article 78 – Discretionary Methods for Administrative Fines ..... 35

Article 79 – Liability for Registry Violations ..... 36

Article 80 – Civil Tort Liability ..... 36



Article 81 – Safe Harbor for Providers of Generative Artificial Intelligence Services ..	37
Article 82 – Liability of Users of Generative Artificial Intelligence .....	37
Article 83 – Liability Exemption for Open-Source AI.....	37
Article 84 – legal Redress .....	38
Article 85 – Public Interest Litigation .....	38
Article 86 – The Interface between Administrative Penalties and Criminal Liabilities .	38
Article 87 – Exemption from Administrative Penalties.....	38
Article 88 – Liability for Failure to Perform Obligations by State Organs .....	38

## **CHAPTER VII SUPPLEMENTARY PROVISIONS ..... 40**

Article 89 – Military Artificial Intelligence.....	40
Article 90 – Definitions .....	40
Article 91 – Implementation Date.....	42
Article 92 – Negative-List Disclosure System .....	42

# CHAPTER I

# GENERAL

# PROVISIONS

## **ARTICLE 1 – LEGISLATIVE BASIS**

This Law is enacted in accordance with the Constitution (of the People's Republic of China) for the purposes of promoting the development of artificial intelligence, regulating its research and development, provision, and use, safeguarding national sovereignty, development and security interests, and protecting the lawful rights and interests of individuals and organizations.

## **ARTICLE 2 – SCOPE OF APPLICATION**

This Law shall apply to the research and development, provision, use, and regulation of artificial intelligence conducted within the territory of the People's Republic of China.

Where the research and development, provision, or use of artificial intelligence is conducted outside the territory of the People's Republic of China, but affects or may affect national security, the public interest, or the lawful rights and interests of individuals or organizations within the People's Republic of China, this Law shall also apply.

### **ARTICLE 3 – GOVERNANCE PRINCIPLE**

The State shall coordinate development and security, uphold the integration of innovation promotion and governance in accordance with the law, and implement inclusive and prudent regulation.

### **ARTICLE 4 – HUMAN-CENTRIC PRINCIPLE**

Activities involving the research and development, provision, and use of artificial intelligence shall adhere to the human-centric principle, be oriented toward the ethical use of intelligence, ensure that human beings retain the capacity to supervise and control artificial intelligence at all times, and consistently aim to promote human well-being as the ultimate objective.

### **ARTICLE 5 – SAFETY/SECURITY PRINCIPLE**

Entities engaged in the research and development, provision, and use of artificial intelligence shall take necessary measures to ensure the safety and security of the artificial intelligence systems being developed, provided, and used, as well as the security of related network data.

### **ARTICLE 6 – PRINCIPLE OF OPENNESS, TRANSPARENCY, AND EXPLAINABILITY**

Entities engaged in the provision of artificial intelligence shall adhere to the principle of openness and appropriately label the content of the artificial intelligence they provide.

Entities engaged in the research and development or provision of artificial intelligence shall adhere to the principles of transparency and explainability, and shall take necessary measures to provide clear explanations regarding the purpose, underlying principles, and effects of the artificial intelligence systems they develop or provide.

### **ARTICLE 7 – PRINCIPLE OF ACCOUNTABILITY**

Entities engaged in the research and development, provision, and use of artificial intelligence shall bear responsibility for their respective activities in research and development, provision, and use.

## **ARTICLE 8 – PRINCIPLE OF FAIRNESS AND EQUALITY**

Entities engaged in the research and development, provision, and use of artificial intelligence shall adhere to the principle of fairness, and shall take effective measures to prevent unreasonable differential treatment of individuals or organizations.

In conducting activities related to the research and development, provision, and use of artificial intelligence, full consideration shall be given to the needs of specific groups, including minors, the elderly, and persons with disabilities.

## **ARTICLE 9 – GREEN PRINCIPLE (OF SUSTAINABILITY)**

The State encourages the application of energy-saving and emission-reduction technologies in the research and development, provision, and use of artificial intelligence, so as to promote the construction of a green and intelligent digital ecological civilization.

## **ARTICLE 10 – PRINCIPLE OF PROMOTING DEVELOPMENT AND INNOVATION**

The State shall support the construction of artificial intelligence infrastructure, promote the open sharing of public computing power, public data, and other relevant public resources, and encourage individuals and organizations to lawfully open and share computing power, data, and other relevant resources.

The State shall encourage the research and development as well as the application of artificial intelligence, protect intellectual property rights in the field of artificial intelligence in accordance with the law, and establish a statutory licensing and fair use system compatible with the development of artificial intelligence. The State shall also support scientific research and cultural and creative activities that make use of AI-generated outputs. The competent authority for intellectual property shall, in accordance with the law, formulate supporting rules for the statutory licensing and fair use regime in the field of artificial intelligence, and shall clarify the mechanisms for the protection of rights and the distribution of benefits in respect of AI-generated outputs based on the principle of fairness and reasonableness.

## **ARTICLE 11 – PRINCIPLE OF ETHICS**

Entities engaged in the research and development, provision, and use of artificial intelligence shall integrate ethical requirements throughout the entire lifecycle of such

activities, and promote responsible innovation and the benevolent use of artificial intelligence.

## **ARTICLE 12 – INTERNATIONAL COOPERATION**

The State shall actively engage in international exchanges and cooperation in the field of artificial intelligence, participate in the formulation and implementation of international rules and standards relating to artificial intelligence, and promote the establishment of an international governance framework and normative standards for artificial intelligence that reflect broad-based consensus.

The State shall improve institutional mechanisms for the introduction of talent, the transfer of technology, and international technological collaboration in the field of artificial intelligence.

## **ARTICLE 13 – COMPETENT AUTHORITIES**

The China Administration of Artificial Intelligence (CAAI), under the leadership of the central leading body for artificial intelligence, shall be responsible for the development and administration of artificial intelligence nationwide. Other relevant departments, as well as relevant departments of the military, shall, in accordance with this Law and other applicable laws and administrative regulations, cooperate closely, strengthen coordination, and perform their respective duties in accordance with the law.

Artificial intelligence authorities and other relevant departments of provinces, autonomous regions, municipalities directly under the central government, cities where the governments of provinces and autonomous regions are located, cities in which special economic zones are located, and other major cities approved by the State Council shall, in accordance with relevant State regulations, be responsible for the development and administration of artificial intelligence within their respective jurisdictions.

## **ARTICLE 14 – COLLABORATIVE CO-GOVERNANCE**

The State shall establish and improve a governance mechanism for artificial intelligence that integrates government regulation, corporate responsibility, industry self-regulation, public oversight, and user self-discipline, so as to promote collaborative governance among diverse stakeholders.

## ARTICLE 15 – LEGALITY AND LEGITIMACY

Entities engaged in the research and development, provision, and use of artificial intelligence shall comply with laws and administrative regulations, respect public order and ethical norms, and observe the following requirements:

- a. Uphold the Core Socialist Values, and shall not generate content prohibited by laws and administrative regulations, including but not limited to content that:
  - incites subversion of State power or the overthrow of the socialist system;
  - endangers national security or interests, or harms the national image;
  - incites secession or undermines national unity and social stability;
  - promotes terrorism or extremism;
  - incites ethnic hatred or discrimination;
  - involves violence, obscenity or pornography;
  - or contains false or harmful information.*
- b. Respect intellectual property rights and business ethics, maintain trade secrets, and refrain from using advantages in algorithms, data, platforms, etc., to engage in monopolistic and unfair competitive practices;*
- c. Protect the rights and interests of consumers and workers in accordance with law, respect the lawful rights and interests of others, and fulfill legal obligations to protect specific groups such as minors, the elderly, and persons with disabilities, and refrain from harming the physical and mental health of others or infringing upon their rights/interests to portrait, reputation, honor, privacy, or personal information.*

# **CHAPTER II**

# **SUPPORT AND PROMOTION OF ARTIFICIAL INTELLIGENCE**

## **ARTICLE 16 – DEVELOPMENT PLAN FOR ARTIFICIAL INTELLIGENCE**

The State shall improve and implement the New-Generation Artificial Intelligence Development Plan, advancing breakthroughs in research and development, product application, and industry cultivation in a coordinated manner, so as to comprehensively support scientific, economic, and social development, as well as national security.

People’s governments at or above the provincial level shall incorporate artificial intelligence development into their respective plans for national economic and social development, and may formulate dedicated artificial intelligence development plans as needed.

## **ARTICLE 17 – CONSTRUCTION OF COMPUTING INFRASTRUCTURE**

The State shall establish a system for the provision of public computing resources for artificial intelligence, promote the construction and utilization of public computing resource platforms, strengthen the scientific allocation of computing power, and provide public computing support for the development of artificial intelligence technologies and industries.

The State encourages and supports higher education institutions, research institutes, enterprises, and other organizations to build artificial intelligence computing infrastructure, engage in market-based transactions of computing resources, and guide the rational and orderly use of computing resources across industries, with a view to improving the efficiency of computing infrastructure utilization.

## **ARTICLE 18 – INNOVATION IN ALGORITHMS AND FOUNDATION MODELS**

The State shall support innovation in artificial intelligence algorithms, encourage the establishment and operation of open-source development platforms, open-source communities, and open-source projects, encourage the establishment of open-source artificial intelligence foundations, and promote the secure and compliant application of open-source software projects.

The State shall support the research and development of vertical models in key sectors and establish a sound system for performance evaluation and safety/security assurance tailored to such models.

Organizations and individuals that make significant contributions to breakthrough research or applied innovation in artificial intelligence technologies shall, in accordance with the law, be commended and rewarded.

Where, in the course of model training, certified de-identification technologies conforming to national standards are used to handle personal information, the entity shall not be subject to the obligations of a personal information handler.



## **ARTICLE 19 – SUPPLY OF DATA AS A FACTOR OF PRODUCTION**

The State shall support the development of foundational and thematic databases in the field of artificial intelligence, promote the efficient aggregation and shared use of data resources, and expand the scope of public data made available for artificial intelligence applications. The State shall comprehensively implement the national integrated big data center system, optimize the layout of data center infrastructure, foster and scale up data center clusters, and establish a system for the reasonable use of training data for artificial intelligence, thereby ensuring the supply of data as a factor of production in the field of artificial intelligence.

The State encourages and guides relevant actors to carry out coordinated research and development in big data and artificial intelligence technologies, supports the deep integration of data with domain-specific knowledge, and promotes the development of data products to serve the needs of algorithm design, model training, product testing, and contextual/scenario-based application.

## **ARTICLE 20 – STATUTORY LICENSING FOR THE USE OF COPYRIGHTED WORKS IN FOUNDATION MODEL TRAINING**

The State shall establish a statutory licensing regime for the use of copyrighted works in the training of foundation models, and shall improve the standards for statutory licensing fees and the mechanisms for royalty allocation.

Where a developer of a foundation model meets the conditions prescribed by the State and obtains the statutory license set forth in the preceding paragraph, they may, without obtaining authorization from the copyright holder, use published works in the course of model training—unless the copyright holder has explicitly stated that such use is not permitted. However, remuneration shall be paid to the copyright holder in accordance with relevant provisions.

## **ARTICLE 21 – FAIR USE OF COPYRIGHTED WORKS IN TRAINING OPEN-SOURCE FOUNDATION MODELS**

Where a developer of an open-source foundation model uses legally obtained copyrighted works in the course of model training, such use may be made without obtaining

authorization from the copyright holder and without payment of remuneration—unless the copyright holder has explicitly stated that such use is not permitted.

Developers of open-source foundation models are encouraged to provide appropriate compensation to copyright holders by reasonable means, so as to promote the dissemination and use of copyrighted works.

## **ARTICLE 22 – ARTIFICIAL INTELLIGENCE PILOT ZONES AND AUTHORIZED LEGISLATURE**

The State may establish artificial intelligence pilot zones in eligible regions to promote experimental and pioneering innovation in artificial intelligence, facilitate the integration of industry, academia, research, and application, and foster an enabling ecosystem for AI development.

The people’s congresses of cities hosting AI pilot zones and their standing committees may, in accordance with this Law and in light of the practical needs of AI innovation and development within the pilot zones, and in compliance with the Constitution as well as the basic principles of laws and administrative regulations, formulate regulations governing the research and development, provision, and use of artificial intelligence, to be applied within the respective pilot zones.

Regulations adopted within AI pilot zones may, pursuant to delegated authority, include adaptive provisions that diverge from national laws, administrative regulations, or local regulations.

Regulations formulated by AI pilot zones shall be filed with the Standing Committee of the National People’s Congress and the State Council for the record. Where such regulations include provisions that adapt or diverge from national laws, administrative regulations, or ministerial rules, the circumstances and justifications for such adaptations shall be provided.

## **ARTICLE 23 – FREE TRADE ZONE EXEMPTIONS**

Upon approval by the State Council, free trade zones (including free trade ports) may implement preferential tax policies and adopt flexible adjustments to measures concerning intellectual property protection, cybersecurity and data governance, and trade controls for eligible activities involving the research and development or provision of

artificial intelligence. These measures aim to promote international technological exchange, cross-border data sharing, and international scientific cooperation.

## **ARTICLE 24 – DYNAMIC ASSESSMENT OF POLICY AND REGULATORY COMPATIBILITY**

The State shall establish a mechanism for assessing the compatibility of policies, decisions, and institutional measures with the development and security landscape of artificial intelligence. Such assessments shall apply to both proposed and existing policies, decisions, and institutional arrangements.

Where an assessment concludes that a given measure may significantly affect the development or security of artificial intelligence, timely adjustments, repeals, or revisions shall be made accordingly.

## **ARTICLE 25 – FISCAL AND PROCUREMENT SUPPORT**

The central government shall establish a dedicated budget line for artificial intelligence within its fiscal budget and allocate special funds for AI development.

People's governments at or above the county level shall, based on actual conditions, allocate special funds for AI development within their respective fiscal budgets.

Governments at all levels, as well as state-owned enterprises and public institutions, are encouraged to procure open-source artificial intelligence products and services that conform to national standards.

## **ARTICLE 26 – TAX CREDITS AND INCENTIVES**

Developers and providers of artificial intelligence may apply tax credits, at a rate not lower than 30 percent, to the amount invested in the development or procurement of dedicated equipment used for safety/security and governance purposes.

The State shall formulate dedicated tax incentive policies for open-source artificial intelligence research and development. Entities engaged in open-source AI R&D that meet the criteria set by the National AI Administrative Authority may, in accordance with the law, enjoy tax incentives such as super-deductions for R&D expenditures.

## **ARTICLE 27 – INDUSTRIAL DEVELOPMENT AND APPLICATION INNOVATION**

Governments and state-owned or public institutions are encouraged to accelerate the transformation and application of key artificial intelligence technologies, promote technological integration and innovation in business models, advance the development of intelligent products in key sectors, actively cultivate emerging AI-driven industries, and foster internationally competitive artificial intelligence industry clusters.

The State shall promote the integrated and innovative application of artificial intelligence across sectors, support pilot and demonstration projects in key industries and fields, facilitate the scaled deployment of artificial intelligence, and encourage the adoption and dissemination of new AI technologies, products, services, and business models.

## **ARTICLE 28 – PROMOTING INNOVATION BY SMALL AND MEDIUM-SIZED ENTERPRISES**

The State encourages small and medium-sized enterprises to engage in the research and development and provision of artificial intelligence, with a particular focus on supporting their technological innovation, product development, and application expansion in the areas of foundation models and their specific applications.

## **ARTICLE 29 – GOVERNMENT-LED PILOT APPLICATIONS**

Government agencies, public institutions, and other organizations lawfully vested with public affairs management functions are encouraged to take the lead in exploring the application of artificial intelligence technologies in areas such as government services and public administration, and to give priority to the procurement and use of safe/secure and reliable AI products and services.

## **ARTICLE 30 – EVALUATION SYSTEMS**

The State shall support and encourage research institutions, universities, enterprises, and public institutions to participate in the development of evaluation systems for artificial intelligence models, promote the creation of fair, reliable, and cost-effective evaluation benchmarks, and develop testing protocols with international competitiveness and interoperability.

## **ARTICLE 31 – TALENT CULTIVATION**

The State shall support institutions of higher education in improving the disciplinary layout and talent cultivation mechanisms in the field of artificial intelligence.

Higher education institutions, research institutes, enterprises, and other relevant entities are encouraged to carry out basic theoretical research and the development of critical and shared technologies addressing major scientific frontiers in the field of artificial intelligence, and to undertake major projects related to scientific and technological advancement and industrial innovation.

The State shall support the establishment of innovative mechanisms for project management, talent evaluation, and the incentivization of technology transfer that are conducive to the development of artificial intelligence.

# CHAPTER III

# ARTIFICIAL

# INTELLIGENCE

# OVERSIGHT

# SYSTEM

## **ARTICLE 32 – CATEGORIZED OVERSIGHT SYSTEM**

The State establishes an Artificial Intelligence Negative List, subjecting products and services within the negative list to a licensing oversight system and, where necessary, those outside the negative list to a registry oversight system.

The National AI Administrative Authority, considering the critical role of AI in economic and social development, and the potential risks to national security, public interests, societal stability, environmental protection, the legitimate rights and interests of individuals and organizations, and the economic order, should it be attacked, tampered with, destroyed, or illegally accessed or utilized, shall take the lead in formulating and periodically updating the Negative List for AI products and services.

## **ARTICLE 33 – NEGATIVE-LIST OVERSIGHT SYSTEM**

Prior to conducting R&D or providing services and products that are within the scope of the Artificial Intelligence Negative List, entities must obtain administrative licenses from the National AI Administrative Authority.

Unlicensed activities, or activities that exceed the scope of the granted license for R&D or provision of products and services within the Artificial Intelligence Negative List, are prohibited.

## **ARTICLE 34 – LICENSING CONDITIONS FOR THE NEGATIVE LIST**

Entities applying for a license to conduct R&D, or to provide services and products within the scope of the Artificial Intelligence Negative List, must meet the following conditions:

- 1. Be a legal entity established in accordance with the laws of the People's Republic of China;*
- 2. The principal person in charge must be a Chinese citizen;*
- 3. Employ full-time personnel with specialized knowledge in quality assurance, safety measures, human oversight, and compliance management that is commensurate with the associated risks;*
- 4. Possess a comprehensive Artificial Intelligence Quality Management System, Network Data Security Management System, and Scientific Ethics Review System;*
- 5. Implement secure and controllable measures to safeguard artificial intelligence technology;*
- 6. Have an emergency response mechanism for artificial intelligence that is proportionate to the associated risks;*
- 7. Possess suitable premises, facilities, and funding that are commensurate with the scale of artificial intelligence R&D, and provision;*
- 8. Comply with other provisions as stipulated by laws and administrative regulations.*

## **ARTICLE 35 – APPLICATION FOR LICENSES WITHIN THE NEGATIVE LIST**

AI developers and providers applying for a license to engage in R&D or provision of AI products and services within the scope of the Negative List must submit the following documentation:

- 1. Application form;*
- 2. Proof of legal entity status, premises, and funding;*
- 3. Verification that the principal person in charge is a Chinese citizen;*
- 4. Credentials of full-time personnel specializing in quality assurance, safety measures, human oversight, and compliance management;*
- 5. Information on the Artificial Intelligence Quality Management System, Network Data Security Management System, Scientific Ethics Review System, and Risk Management System, as well as their implementation status;*
- 6. Artificial Intelligence Safety/Security Assessment Report;*
- 7. Any other documentation as required by applicable laws and administrative regulations.*

## **ARTICLE 36 – APPROVAL OF LICENSES WITHIN THE NEGATIVE LIST**

Upon receiving an application for a license for R&D or provision of AI products and services within the scope of the Negative List, the National AI Administrative Authority must conduct a preliminary review within 10 days.

If, upon preliminary review, it is found that the submitted application materials from the AI developers and providers do not meet the required criteria, the National AI Administrative Authority may request that they supplement or correct the application. If the AI developers and providers do not provide the required supplementary materials or corrections without legitimate reason, the application will be deemed withdrawn.

If the preliminary review establishes that all submitted materials are complete, the National AI Administrative Authority must finalize its review within 45 days of accepting the application, and render a decision either to grant or deny the license. If approved, a license for R&D or provision of AI will be issued to the applicant; if denied, the applicant must be notified in writing with reasons for the denial provided.



Should the National AI Administrative Authority be unable to make a decision after the expiration of the period, an extension of up to 10 days may be granted upon approval by the Head of the National AI Administrative Authority. The reason for such an extension must be communicated to the applicant.

### **ARTICLE 37 – REAPPLICATION FOR LICENSES WITHIN THE NEGATIVE LIST**

The license for R&D or provision of Artificial Intelligence within the scope of the Negative List should specify the duration and scope of the license’s validity.

If activities exceed the scope of the license or if changes in technology, use case scenarios, or target user groups lead to a change in associated risks, AI developers and providers within the scope of the Negative List must reapply for a license for R&D or provision.

Six months prior to the expiration of the license, AI developers and providers within the scope of the Negative List may apply for a renewal of their license for R&D or provision.

Should AI developers and providers within the scope of the Negative List cease their licensed R&D or provision activities, they are required to apply for cancellation of the license with the National AI Administrative Authority within three months from the date of cessation.

### **ARTICLE 38 – PUBLIC DISCLOSURE OF LICENSE**

AI developers and providers within the scope of the Negative List must prominently display the license number in the AI products or services they provide.

### **ARTICLE 39 – COMPLAINT, REPORTING, AND CLARIFICATION MECHANISMS**

Individuals and organizations that discover unlawful activities in the R&D or provision of Artificial Intelligence within the scope of the Negative List have the right to file complaints or reports with the National AI Administrative Authority. The said Authority must promptly verify and address such complaints or reports.

Individuals and organizations that have questions or concerns regarding the activities of R&D or provision of AI within the scope of the Negative List have the right to request

clarification from the National AI Administrative Authority. The said Authority must promptly respond and address the matters raised.

## **ARTICLE 40 – OTHER LICENSES AND REGISTRIES**

Where laws or administrative regulations stipulate that the application of artificial intelligence shall be subject to administrative licensing or registry, AI providers and users shall legally obtain the licenses or complete registries/filings in accordance with the law.

# **CHAPTER IV**

# **OBLIGATIONS OF**

# **AI DEVELOPERS**

# **AND PROVIDERS**

## **SECTION 1: GENERAL PROVISIONS**

### **ARTICLE 41 – SAFETY/SECURITY OBLIGATIONS**

AI developers and providers shall conduct safety/security assessments prior to deployment or market release, and periodically throughout the provision of products or services, in order to prevent security risks and ensure the safe and stable operation of artificial intelligence throughout its lifecycle in alignment with its intended purpose. Safety/security assessment reports shall be retained for no less than five years.

AI developers and providers shall promptly publish best practices for safety/security, and guide users in the safe and proper use of artificial intelligence.

AI developers and providers shall comply with the requirements of this Law regarding logging, technical documentation, and related obligations, and shall ensure traceability, such that, in the event of an incident, problems can be promptly and accurately traced and located to ensure safety/security.

AI developers and providers shall take effective measures to improve the accuracy and reliability of content generated by models.

## **ARTICLE 42 – OBLIGATION TO MANAGE SECURITY VULNERABILITIES**

Relevant organizations and individuals are encouraged to notify AI developers and providers of any security vulnerabilities present in their products or services.

AI developers and providers must fulfill their obligations to manage security vulnerabilities in accordance with relevant regulations, ensure that such vulnerabilities are promptly rectified and reasonably disclosed, and guide and support users in taking preventative measures.

## **ARTICLE 43 – OBLIGATION TO AUDIT**

AI developers and providers shall, in accordance with relevant State regulations and the requirements of the National AI Administrative Authority, conduct audits to verify the compliance of input data, algorithmic models, and output data. They shall review and evaluate whether the provision of AI products and services complies with applicable laws and administrative regulations.

## **ARTICLE 44 – OBLIGATION TO REMEDY AND NOTIFY**

AI developers and providers shall strengthen risk monitoring concerning infrastructure security, algorithm and model safety/security, and data security. Upon discovering security vulnerabilities, flaws, or logical defects, they shall immediately take remedial measures.

Where a developer becomes aware of a security incident involving the AI it has developed, it shall immediately take response measures and notify the provider. The provider shall fulfill its notification obligations as set out in Paragraph 3 of this Article. Where a provider becomes aware of a security incident involving the AI it provides, it

shall likewise take immediate response measures, fulfill the notification obligations set out in Paragraph 3, and promptly notify the developer.

AI providers shall promptly take response measures and, in accordance with relevant State regulations, inform users and report to the competent authorities the following:

- a. The occurrence and impact scope of the safety incident;*
- b. The remedial actions already taken by the AI provider, as well as potential actions that users can take to mitigate harm;*
- c. The contact information of the AI provider.*

Where the provider's measures are sufficient to effectively prevent substantial harm to users, user notification may be waived. However, where the National AI Administrative Authority determines that harm may still result, it may require the provider to notify affected users.

Where a developer discovers a security incident or receives notification of such from a provider, it shall immediately conduct an assessment. If the assessment reveals risks or defects originating from the development stage, the developer shall promptly notify other providers, and suspend or withdraw the relevant AI products or services until the risks have been resolved. Providers so notified shall immediately take response measures to manage the risks associated with their products or services.

## **ARTICLE 45 – OBLIGATION OF OPENNESS AND TRANSPARENCY**

Where AI providers offer services involving interaction with natural persons, they shall, prior to user engagement, inform such individuals—using concise, clear, and intelligible language—that they are interacting with an AI service. However, if a natural person is able to discern from the context that they are interacting with an AI service, such notice is not required.

Providers of deep synthesis services shall, in accordance with relevant State regulations, apply reasonable labeling to synthesized content and provide public notice regarding the use of deep synthesis technologies. Providers offering algorithmic recommendation services shall publicly disclose relevant rules governing such services and take measures to improve transparency.

Prior to the market launch or provision of services, AI providers shall inform users, through appropriate means, of the following:

- a. The basic principles, intended purpose, and main operating mechanisms of the product or service;*
- b. Public information on the license or registry of the product or service;*
- c. The rights and remedies available to the user;*
- d. Any other information required by laws or administrative regulations.*

AI developers should cooperate with providers to fulfill these obligations above.

## **ARTICLE 46 – OBLIGATION OF EXPLAINABILITY**

For AI products and services that have a significant impact on individual rights and interests, users of the AI have the right to request explanations from the providers about the decision-making process and methods of the products and services. Users have the right to lodge complaints about unreasonable explanations.

AI providers should take into account factors such as the scenarios and nature of their products and services, as well as the level of technological development in the industry, and promptly respond to users' requests.

AI developers should cooperate with providers to fulfill these obligations above.

## **ARTICLE 47 – OBLIGATION OF FAIRNESS**

AI developers should take proportionate and necessary measures during the processes of data handling and labeling, algorithmic model design, development, and validation testing to effectively prevent harmful biases and discrimination.

AI providers should enhance the stewardship of input and output data while providing products and services to effectively prevent harmful biases and discrimination.

## **ARTICLE 48 – RISK MANAGEMENT**

AI providers, taking into consideration factors such as the scenarios, nature, audience, and the level of technological development within the industry, should establish and implement a comprehensive risk management system that spans the entire lifecycle. Prior to the deployment and during the use of their products and services, AI providers must identify potential risks associated with artificial intelligence and implement necessary

control measures. AI providers are required to maintain records of risk identification and the measures taken for no less than two years.

AI developers must establish and operate a risk management system throughout the R&D process, including design, data collection and training, model selection, and testing and validation. They should identify risks associated with artificial intelligence and implement necessary control measures. While ensuring the confidentiality of trade secrets, AI developers should cooperate by providing safety/security assessment reports, records of risk identification, and control measures to support AI providers in fulfilling their risk management obligations for AI services. AI providers must retain records of risk assessments and the measures taken for no less than two years.

## **ARTICLE 49 – OBLIGATION OF AI ETHICS REVIEW**

AI developers, providers, and users that meet the conditions specified by the National AI Administrative Authority shall establish ethics review mechanisms for artificial intelligence and carry out ethics reviews in accordance with relevant State regulations.

Where the research, development, provision, or use of artificial intelligence is conducted in the fields of government affairs or public service, ethics review mechanisms shall be established and ethics reviews shall be conducted in accordance with relevant State regulations.

The State encourages the establishment of third-party ethics review institutions to provide ethics review services for small and medium-sized enterprises that have not established their own ethics review committees, in accordance with relevant State regulations.

## **ARTICLE 50 – OBLIGATIONS OF STATE ORGANS IN PROVISION AND DEVELOPMENT**

Where State organs and other organizations lawfully vested with public affairs management functions engage in the research, development, or provision of artificial intelligence in areas such as government services or public administration, they shall comply with the obligations applicable to AI developers and providers under this Law. In particular, they shall ensure the security, transparency, and fairness of artificial intelligence used in the management of public affairs.

## **ARTICLE 51 – DESIGNATED REPRESENTATIVES**

AI developers and providers located outside the territory of the People’s Republic of China, as specified in Paragraph 2 of Article 2 of this Law, shall establish a dedicated office within the territory of the People’s Republic of China or designate a representative to handle matters related to artificial intelligence. The name of the office or the name and contact information of the designated representative shall be filed with the National AI Administrative Authority.

## **ARTICLE 52 – TRUSTED DATA**

The State shall support the establishment of authoritative and secure information databases and the development of a labeling system to assess and indicate the trustworthiness of different types of data.

## **SECTION 2: OBLIGATIONS OF ARTIFICIAL INTELLIGENCE DEVELOPERS**

### **ARTICLE 53 – ENHANCED OBLIGATIONS FOR AI DEVELOPERS ON THE NEGATIVE LIST**

AI developers falling under the Negative List are obligated to comply with the following requirements:

- a. Develop and maintain technical documentation that meets the requirements of this law;*
- b. During the R&D process, establish and operate a quality management system that conforms to the requirements of this law, and cooperate with providers in fulfilling relevant duties;*
- c. Cooperate with providers in fulfilling relevant duties;*
- d. Comply with other obligations as stipulated by laws and administrative regulations.*

### **ARTICLE 54 – SPECIAL OBLIGATIONS FOR DEVELOPERS OF FOUNDATION MODELS**

Developers of foundation models should abide by the following requirements:



1. **Security and Risk Management:** Establish and maintain a robust security risk management system in accordance with national regulations, promptly and effectively preventing, monitoring, and handling risks that may affect national security, public interests, or the legitimate rights and interests of individuals, organizations, and economic order.
2. **Model and Data Stewardship:** Establish and maintain a comprehensive model and data stewardship system for foundational models in accordance with national regulations.
3. **Openness, Fairness, and Justice Principles:** Follow the principles of openness, fairness, and justice in formulating usage rules for foundational models, clarifying the obligations of developers and providers of foundational models, and preventing the abuse of market dominance.
4. **Compute:** Ensure the investment of computing resources necessary for managing safety/security risks.
5. **Assistance:** Assist other developers and providers in fulfilling their obligations as specified by this law.
6. **Sanctions for Violations:** For developers and providers who seriously violate the provisions of this law, take necessary measures such as suspending services.
7. **Public Oversight:** Establish an independent institution mainly composed of external members to supervise the development of foundational models; publish an annual social responsibility report and accept public supervision.

## SECTION 3: OBLIGATIONS OF ARTIFICIAL INTELLIGENCE PROVIDERS

### ARTICLE 55 – REGISTRY OBLIGATIONS

AI providers offering products or services not listed on the negative list, with registered user numbers exceeding one million, should, within ten working days from the date of meeting the conditions, register the following information with the National AI Administrative Authority:

- a. **Contact Information:** Name or business name and contact details of the AI provider.

- b. **Details of AI Product/Service:** Trademarks or names, the form of provision, application areas, algorithm types, and a self-assessment report on security.*
- c. **Content to be Publicized in the Record:** Information that is intended to be made public as part of the registration.*
- d. **Other Information:** Any other information required by laws or administrative regulations.*

Those with registered user numbers exceeding ten thousand but less than one million should, within ten working days from the date of meeting the conditions, register the aforementioned information with the provincial-level authority in charge of artificial intelligence.

Should there be any changes to the registered information, they must be amended within ten working days from the date of the change.

AI providers that have completed the registry shall indicate the filing number in a prominent position on their websites, applications, etc., on which services are provided to the public.

## **ARTICLE 56 – REGISTRY PROCESS**

Upon receiving the registration materials, if the materials are complete, the regulatory authority should register them within thirty working days, issue a registration number, and make a public announcement. If the materials are incomplete, the regulatory authority must notify the registrant to provide additional materials within ten working days.

## **ARTICLE 57 – INTERNAL MANAGEMENT SYSTEMS**

AI providers should take the following measures to ensure that AI complies with laws and administrative regulations:

- a. **Establish internal systems and corresponding operational procedures for data security, risk control, and quality management;***
- b. **Keep logs automatically generated during the provision of AI products and services;***
- c. **Regularly conduct education and training for employees;***
- d. **Adopt compliant technical measures to ensure robustness and resistance to attacks;***

- e. Conduct an AI audit at least every two years;*
- f. Other measures as stipulated by laws and administrative regulations.*

## **ARTICLE 58 – TERMINATION MECHANISM**

When an AI provider terminates the provision of products or services, the following appropriate arrangements should be made:

- a. Publicize the termination plan and user rights at least 30 working days in advance;*
- b. Delete users' personal information within 30 working days from the date of termination. According to relevant national regulations, necessary handling of data generated during the provision of AI products and services, training data, and algorithmic models should be carried out;*
- c. Other measures as stipulated by laws and administrative regulations.*

## **ARTICLE 59 – PERMISSION REVOCATION**

AI providers within the Negative List should notify the competent authority at least 30 working days in advance, providing relevant details, and return the license to the original licensing authority after terminating the service.

AI providers outside the Negative List should complete the procedures for revoking the registry within 20 working days from the date of terminating the service.

## **ARTICLE 60 – ENHANCED OBLIGATIONS FOR NEGATIVE-LISTED AI PROVIDERS**

AI providers within the scope of the Negative List shall also fulfill the following obligations:

- a. Conduct safety/security assessments in accordance with the requirements of this law to ensure that operations are safe and robust;*
- b. Develop and retain technical documentation that complies with the requirements of this law, to demonstrate that the provided AI systems meet the law's stipulations for AI systems on the Negative List;*
- c. Establish and operate a full-lifecycle quality management system that conforms to the requirements of this law;*

- d. Ensure that during the autonomous operation of AI products and services, humans have the ability to intervene or take control at any time;*
- e. Other obligations stipulated by laws or administrative regulations.*

## **ARTICLE 61 – OBLIGATIONS FOR PLATFORM OPERATORS**

If operators of online platforms are aware, or should be aware, that providers of products or services on the platform engage in AI provision through the platform, they should legally establish or amend their terms of service and transaction rules. They must clarify the standards and obligations for providers of products or services on the platform that offer artificial intelligence, ensuring that these providers do not abuse a dominant market position.

## **ARTICLE 62 – SECURITY OF TERMINAL DEVICE PERMISSIONS**

Providers of AI terminal devices shall ensure the quality of terminal device products. Providers of AI services embedded in terminal devices shall ensure the security and transparency of such services.

Where AI services on terminal devices involve cross-application permission invocation, the principle of minimum necessity shall be followed, and a dynamic authorization mechanism shall be implemented. The scope of user authorization shall be limited to the specific functional requirements of the given scenario, and generalized authorization practices that result in the acquisition of unrelated permissions shall be prohibited.

# CHAPTER V

# COMPREHENSIVE AI GOVERNANCE MECHANISM

## ARTICLE 63 – RESPONSIBILITIES OF THE NATIONAL AI ADMINISTRATIVE AUTHORITY

The National AI Administrative Authority shall exercise the following administrative responsibilities for AI in accordance with the law:

- 1. Submit a special report on the development and governance of AI to the State Council by March 31 of each year;*
- 2. Conduct education and promotion for AI ethics and safety/security, and provide guidance and supervision for the research & development, provision, and usage of AI;*
- 3. Formulate AI regulatory rules and guidelines, and organize the development of standards concerning AI ethics, safety, and management;*
- 4. Promote the construction of a socialized service system for artificial intelligence governance, guide and support professional institutions in*

- providing services such as artificial intelligence safety/security and ethics monitoring, evaluation, auditing, and certification;*
- 5. Guide and support the development and activities of open-source artificial intelligence innovation communities; and steer and coordinate such communities in the regular releases and updates of best practice guidelines for open-source AI projects;*
  - 6. Establish an artificial intelligence ethics and risk monitoring and early-warning mechanism, and organize the acquisition, analysis, research and early-warning of ethics and risk information in the field of artificial intelligence;*
  - 7. Establish an emergency response mechanism for AI ethics and safety/security incidents;*
  - 8. Receive and handle complaints and reports related to the research & development, provision, and usage of AI technologies and products;*
  - 9. Investigate and address unlawful activities in the research, development, provision, and usage of artificial intelligence, as well as ethically problematic conduct that may lead to serious consequences;*
  - 10. Other responsibilities stipulated by laws or administrative regulations.*

## **ARTICLE 64 – AI ETHICS EXPERT COMMITTEES**

The National AI Administrative Authority shall establish a National AI Ethics Expert Committee, and local AI regulatory authorities shall establish AI ethics expert committees at their respective levels.

The National AI Ethics Expert Committee shall study major ethical issues arising in the research, development, provision, and use of artificial intelligence, provide advisory opinions to the National AI Administrative Authority, and guide ethics review-related work nationwide.

Local AI ethics expert committees shall study ethical issues arising within their respective administrative jurisdictions during the research, development, provision, and use of artificial intelligence, provide advisory opinions to their corresponding local AI regulatory authorities, and guide the work of AI ethics review committees established by developers, providers, and users within their jurisdictions.

## **ARTICLE 65 – SECURITY REVIEW SYSTEM**

Where activities involving the research, development, provision, or use of artificial intelligence affect or may affect national security, a security review shall be conducted in accordance with relevant State regulations.

Decisions made in accordance with the security review process specified in laws shall be considered final.

## **ARTICLE 66 – TIMEFRAME FOR PRELIMINARY PROCEDURES**

When AI developers, providers, or users apply for safety/security reviews, registries, or administrative licenses for new artificial intelligence technologies or applications in accordance with this Law and relevant national regulations, the National AI Administrative Authority shall process and respond within the prescribed timeframe.

## **ARTICLE 67 – INTERVIEWING**

If the National AI Administrative Authority and local AI administrative authorities at all levels, in the course of fulfilling their responsibilities, discover that activities related to the R&D or provision of AI pose significant risks or have resulted in safety/security incidents, they may, in accordance with specified authorities and procedures, interview the relevant AI developers or providers and require them to take the following measures:

- a. Implement corrective actions as specified to eliminate potential risks;*
- b. Provide an appropriate explanation of their R&D, and provisioning activities, clarify responsibilities related to the development, management, and operation of AI services, discuss measures taken to ensure fairness, safety, and stability, and assess the impact on stakeholders;*
- c. Commission a professional organization to conduct a compliance audit of their AI R&D and provisioning activities.*

If AI developers and providers commit to timely corrective actions to achieve compliance, and can effectively avoid causing harm through their AI R&D, provision, or usage activities, they may not be required to suspend relevant activities. However, if the National AI Administrative Authority deems that potential harm may occur, it may order the suspension of such activities.

## **ARTICLE 68 – INNOVATIVE REGULATION**

In cases where minor violations occur in the activities related to the R&D, provision, and use of AI, and the decides not to administer administrative penalties according to the law, the Authority should adopt measures such as criticism and education, guidance interviews, and organizing consultative meetings to encourage the parties involved to conduct their activities – R&D, provision, and use in the AI industrialization in a lawful and compliant manner.

The National AI Administrative Authority shall formulate dedicated compliance guidelines for open-source artificial intelligence developers, promoting the innovative development of open-source artificial intelligence.

## **ARTICLE 69 – REGULATORY SANDBOX**

The National AI Administrative Authority shall establish an AI regulatory experimental mechanism and issue specific regulations and guidelines concerning the following matters:

- a. Conditions for participating in the regulatory experimentation;*
- b. Operational mechanisms of the regulatory experimentation;*
- c. Risk monitoring and prevention measures in the regulatory experimentation;*
- d. Obligations and liability reduction mechanisms for AI developers and providers participating in the regulatory experimentation.*

## **ARTICLE 70 – INTERNAL WHISTLEBLOWER PROTECTION AND REPORTING MECHANISM**

AI developers, providers, and users shall establish and improve internal whistleblower systems and whistleblower protection mechanisms, and clarify procedures and requirements for handling reports.

The scope of reporting includes, but is not limited to, the following circumstances occurring during the research, development, provision, or use of artificial intelligence:

- a. Potential safety hazards that may cause significant bodily injury or property loss;*
- b. Violations of legally prescribed risk prevention obligations or safety requirements;*



- c. Intentional concealment or distortion of significant technical defects or the results of safety assessments;*
- d. Other circumstances that may affect national security or public safety.*

Where an internal whistleblower reports to their organization, or to the competent regulatory authority or judicial authority, the organization to which the developer, provider, or user belongs shall not retaliate against the whistleblower in any form.

Where a developer, provider, or affiliated institution identifies and eliminates safety hazards, or prevents or mitigates harmful consequences in a timely manner as a result of a whistleblower's report, such conduct shall be considered a circumstance warranting mitigation or reduction of administrative penalties. If a whistleblower was involved in the relevant violation but voluntarily reports and actively cooperates with the investigation, their liability may be mitigated, reduced, or exempted in accordance with the law.

The National AI Administrative Authority shall establish reporting channels, promptly accept and handle reports, and maintain the confidentiality of the personal information and content of whistleblowers. The State shall protect the personal information, privacy, and safety of internal whistleblowers. No organization or individual may disclose the identity or personal information of an internal whistleblower, nor may they threaten, intimidate, or retaliate against such whistleblower.

## **ARTICLE 71 – OFFICIALS RESPONSIBLE FOR STATE ORGANS**

State organs and other organizations, which are legally endowed with the management of public affairs, shall designate individuals responsible for artificial intelligence. These appointed persons are tasked with supervising the use of artificial intelligence and the implementation of safety protection measures.

## **ARTICLE 72 – LAW ENFORCEMENT**

The National AI Administrative Authority should enhance the development of specialized teams and specialized technology, improve the staff's professional capabilities, conduct relevant technical training, and continuously elevate the capability and standard of AI regulation.

Furthermore, the National AI Administrative Authority should, in accordance with the law, establish administrative enforcement procedures specific to its system and set up a system for supervising administrative enforcement.

## **ARTICLE 73 – GOVERNANCE THROUGH TECHNOLOGY**

The State shall support enterprises, research institutions, and other organizations in researching and developing technologies related to AI monitoring and early warning, safety/security assessment, and emergency response. It encourages the application of regulatory technology (RegTech) and compliance technology (ComplianceTech) in the field of artificial intelligence.

## **ARTICLE 74 – COUNTERMEASURES AGAINST FOREIGN ENTITIES**

Where overseas organizations or individuals engage in AI R&D, provision, or usage activities that infringe upon the legitimate rights and interests of citizens of the People's Republic of China, or endanger the national security or public interests of the People's Republic of China, the National AI Administrative Authority may, in accordance with the law, adopt measures to restrict or prohibit their AI R&D, provision, or usage activities within the territory of the People's Republic of China and shall make public announcements thereof.

## **ARTICLE 75 – RECIPROCAL MEASURES**

If any country or region adopts discriminatory prohibitions, restrictions, or similar measures against the People's Republic of China in aspects related to AI R&D, investment, trade, etc., the People's Republic of China may take reciprocal measures against that country or region based on the actual circumstances.

# CHAPTER VI

# LIABILITIES

## ARTICLE 76 – GENERAL LIABILITIES

Where any entity engages in the research, development, or provision of artificial intelligence in violation of this Law, or retaliates against an internal whistleblower, the National AI Administrative Authority shall order rectification, issue a warning, confiscate any illegal gains, and may order the suspension or termination of relevant business activities. Where the entity refuses to rectify, a fine of not more than RMB 1 million may be imposed. The directly responsible persons in charge and other directly liable individuals shall be fined between RMB 10,000 and RMB 100,000.

Where the above-mentioned violations are of a serious nature, the National AI Administrative Authority shall order rectification, confiscate any illegal gains, and impose a fine of not more than RMB 10 million or not more than 4% of the violator's revenue from the previous fiscal year. The Authority may also order the suspension of relevant business operations, require rectification, notify the competent licensing authority to revoke relevant business licenses, or order the revocation of the business license. The directly responsible persons in charge and other directly liable individuals shall be fined between RMB 100,000 and RMB 1 million.

## **ARTICLE 77 – REVOCATION OF NEGATIVE-LIST LICENSES**

Where an artificial intelligence developer or provider violates the provisions of this Law during R&D or provision activities, resulting in a significant safety/security incident, multiple safety/security incidents, or multiple administrative penalties, the National AI Administrative Authority may suspend the license and order rectification within a prescribed period; if rectification is not made upon the expiration of the period, or if a safety/security incident occurs again or an administrative penalty is imposed after the suspension of the license, the National AI Administrative Authority may revoke the license.

## **ARTICLE 78 – DISCRETIONARY METHODS FOR ADMINISTRATIVE FINES**

Fines stipulated in this law may serve as a supplement to or substitute for corrective measures. When the National AI Administrative Authority determines the amount of an administrative fine, it shall adhere to the principles of legality, proportionality, fairness and justice, integration of punishment and education, and comprehensive discretion. The following factors should be fully considered:

- 1. The nature, severity, duration, and impact of the violation, as well as the extent and degree of damage caused;*
- 2. Whether the violation was intentional or negligent;*
- 3. Whether remedial measures have been taken to mitigate the potential loss caused by the violation;*
- 4. Whether the National AI Administrative Authority was notified in accordance with the provisions of this law;*
- 5. Whether reasonable and effective organizational and technical measures have been taken to manage the risks of AI in accordance with this law;*
- 6. Whether compliance with AI and safety-related standards has been achieved or relevant certifications have been obtained;*
- 7. Prior violations;*
- 8. The impact of internal whistleblowing on the occurrence or severity of the damage or harm;*
- 9. Other factors stipulated by laws and regulations that may aggravate or mitigate the penalty.*

## **ARTICLE 79 – LIABILITY FOR REGISTRY VIOLATIONS**

If an AI provider is required to file a registry but fails to do so, the National AI Administrative Authority shall issue a warning. In severe cases, a fine between ten thousand and one hundred thousand yuan may be imposed.

If an AI provider obtains registry through improper means, such as concealing relevant information or providing false materials, the National AI Administrative Authority shall revoke the registry, issue a warning, and make a public criticism. In severe cases, a fine between one hundred thousand and one million yuan may be imposed.

If an AI provider terminates its service without going through the procedures to cancel the registry, or if it is subjected to administrative penalties such as being ordered to shut down the website, having its relevant business permit revoked, or having its operation license revoked due to serious legal violations, the National AI Administrative Authority shall cancel the registry.

## **ARTICLE 80 – CIVIL TORT LIABILITY**

Where the R&D or provision of AI infringes upon individual rights and causes harm, the developer or provider shall bear tort liability, including compensation for damages, unless they can prove the absence of fault.

The compensation under the preceding paragraph shall be determined based on the loss suffered by the user or affected individual or organization, or the benefit obtained by the developer or provider. Where it is difficult to determine either the loss or the benefit, the compensation amount shall be determined in light of the actual circumstances. Where the developer or provider can demonstrate that the harm resulted from the user's intentional circumvention of safety measures and that they fulfilled their corresponding technical protection obligations, their liability may be mitigated.

Where the enterprise or institution to which the developer or provider belongs retaliates against an internal whistleblower—such as by unlawfully terminating their labor contract or taking other adverse measures—compensation of no less than two times and no more than ten times the actual loss shall be paid to the whistleblower, with a minimum amount not less than six months of wages. Where the circumstances are serious, additional compensation and damages for emotional distress may be awarded.

## **ARTICLE 81 – SAFE HARBOR FOR PROVIDERS OF GENERATIVE ARTIFICIAL INTELLIGENCE SERVICES**

Where a provider uses generative artificial intelligence technologies to offer services that generate content such as text, images, audio, or video for the public within the territory of the People’s Republic of China, and satisfies all of the following conditions, it shall not bear liability for compensation in cases of intellectual property infringement:

- a. It has established an effective mechanism for intellectual property complaints, enabling rights holders to safeguard their lawful rights and interests;*
- b. It provides notice to users, through user agreements or other means, that they must not infringe upon the intellectual property rights of others;*
- c. It has adopted rules for the protection of intellectual property rights and, where a user infringes upon the rights of others through the use of generative AI services, it takes lawful and contractual measures such as issuing warnings, restricting functionality, suspending or terminating services;*
- d. It labels AI-generated content in accordance with the law.*

## **ARTICLE 82 – LIABILITY OF USERS OF GENERATIVE ARTIFICIAL INTELLIGENCE**

Where a user infringes upon the intellectual property rights of others through the use of generative artificial intelligence services and is at fault, the user shall bear tort liability.

Where a provider knew or ought to have known that a user was using its services to infringe upon the intellectual property rights of others and failed to take necessary measures, the provider shall bear joint and several liability with the user.

## **ARTICLE 83 – LIABILITY EXEMPTION FOR OPEN-SOURCE AI**

Where individuals or organizations provide certain code modules necessary for AI development on a free and open-source basis, and clearly disclose their functions and associated safety/security risks, they shall not bear legal liability.

Where individuals or organizations provide artificial intelligence on a free and open-source basis and can demonstrate that they have established an AI compliance and governance framework in conformity with national standards and have adopted corresponding safety/security governance measures, their legal liability may be mitigated or waived.

## **ARTICLE 84 – LEGAL REDRESS**

Citizens, legal persons, or other organizations that disagree with the administrative actions taken by the competent authorities for artificial intelligence may apply for administrative reconsideration or file an administrative lawsuit in a People’s Court in accordance with the law.

## **ARTICLE 85 – PUBLIC INTEREST LITIGATION**

Where an artificial intelligence provider violates the provisions of this Law by providing products or services that infringe upon the rights and interests of numerous individuals, the People’s Procuratorates, consumer organizations stipulated by law, and organizations designated by the National AI Administrative Authority may file lawsuits with the People’s Courts in accordance with the law.

## **ARTICLE 86 – THE INTERFACE BETWEEN ADMINISTRATIVE PENALTIES AND CRIMINAL LIABILITIES**

Violations of the provisions of this law that constitute violations of public security administration shall be punished in accordance with the law. If a crime is constituted, criminal liability shall be pursued in accordance with the law.

## **ARTICLE 87 – EXEMPTION FROM ADMINISTRATIVE PENALTIES**

Where artificial intelligence developers or providers commit minor violations and promptly rectify them without causing harmful consequences, no administrative penalties shall be imposed. In cases of first-time violations with minor harmful consequences that are promptly rectified, administrative penalties may be waived.

## **ARTICLE 88 – LIABILITY FOR FAILURE TO PERFORM OBLIGATIONS BY STATE ORGANS**

State organs engaged in the R&D, provision, and use of artificial intelligence shall strictly comply with the obligations defined by this law. Failure to perform the obligations stipulated by this law shall be corrected by its higher-level organ or the National AI Administrative Authority; legal disciplinary action shall be taken against those directly in charge and other directly responsible personnel.

State employees who neglect their duties, abuse their powers, or engage in corruption without constituting a crime shall be disciplined in accordance with the law.

In cases that do not constitute by-law faults of administrative enforcement, the administrative enforcement liability of relevant personnel will not be pursued.



# CHAPTER VII

# SUPPLEMENTARY

# PROVISIONS

## ARTICLE 89 – MILITARY ARTIFICIAL INTELLIGENCE

The regulations governing the R&D, provision, and use of artificial intelligence by the Chinese People’s Liberation Army and the Chinese People’s Armed Police Force shall be separately stipulated by the Central Military Commission in accordance with the principles prescribed in this Law.

## ARTICLE 90 – DEFINITIONS

The following terms in this law have the definitions as described below:

- a. Artificial Intelligence refers to automated systems that operate with a certain level of autonomy, serving specific or general objectives and capable of affecting physical or virtual environments through prediction, recommendation, or decision-making. This includes data, features, models, service provision interfaces, and embedded terminal devices.*

- b. **Open-Source Artificial Intelligence** refers to AI systems that are released to the general public in an accessible form under open-source license frameworks. The technical components of such systems shall include, in accessible form, core elements such as foundation model weights and parameters. Depending on the technical characteristics, they shall also be accompanied by appropriately disclosed training datasets, complete descriptions of model parameters, or corresponding safety/security and compliance documentation. The degree of openness of open-source AI shall meet the practical needs of lowering barriers to technological reuse, enabling local deployment, and permitting freedom of modification, and shall not contravene other applicable laws or regulations.
- c. **Terminal Devices** refer to network-enabled terminal products—such as mobile phones and computers—that are capable of connecting to the internet, equipped with operating systems, and allow users to install application software independently.
- d. **Internal Whistleblowers** refer to natural persons who are currently or were formerly employed by an organization to which an AI developer, provider, or user belongs, and who acquire relevant information in the course of their work and report it.
- e. **Artificial Intelligence Developers** refer to individuals or organizations solely engaged in activities such as algorithm design, training data labeling, feature extraction, model training and optimization, testing deployment, and the free and open-source provision during artificial intelligence research and development.
- f. **Artificial Intelligence Providers** refer to individuals or organizations that provide AI or related technical support for commercial purposes, or regardless of commercial intent, offer AI or related technical support to the public. This does not include individuals or organizations that provide AI for free and as open-source.
- g. **Artificial Intelligence Users** refer to individuals or organizations that utilize AI according to its capabilities and purposes.
- h. **Foundation Models** refer to artificial intelligence models that have undergone training with the accumulation of computing power investment to a certain scale, serving general purposes, and capable of providing technological support for a wide range of downstream services. The floating-point operations (FLOPs) and other computing power standards for the identification of foundation models shall

*be formulated, publicly issued, and regularly updated by the National AI Administrative Authority.*

## **ARTICLE 91 – IMPLEMENTATION DATE**

This law shall come into effect on [Day] [Month] [Year].

## **ARTICLE 92 – NEGATIVE-LIST DISCLOSURE SYSTEM**

The National AI Administrative Authority shall publish the Artificial Intelligence Negative List no later than six months before the implementation of this law, and promptly make it public after periodic updates.