THE MODEL ARTIFICIAL INTELLIGENCE LAW

MAIL v.4.0

Funded by the Special Incubation Program of the *"AI Security Governance Research Laboratory"*, Chinese Academy of Social Sciences

MAY 2026

THE DRAFTING TEAM

CHIEF EXPERT

- ***Honglei LI**, Professor of Law and Chairman of the Joint Board of the Institute of Law and the Institute of International Law, CASS*

THE COORDINATOR

- ***Hui ZHOU**, Deputy Director (Acting Director), Department of Cyber and Information Law, Institute of Law, Chinese Academy of Social Sciences (CASS)*
- ***Yanfeng LI**, Director and Senior Editor, 8th Editorial and Research Department, Institute of Information Studies, CASS*

DRAFTING GROUP EXPERTS (In alphabetical order of surnames by pinyin)

- ***Yanlin CAO**, Director and Research Fellow, Medical and Health Law Office, Institute of Medical Information, Chinese Academy of Medical Sciences*
- ***Tianhao CHEN**, Tenured Associate Professor, School of Public Policy and Management, Tsinghua University*
- ***Xingsi DI**, Assistant Professor, School of Law, Guangzhou University; Distinguished Researcher, Guangdong-Hong Kong-Macao Greater Bay Area Legal System Research Center, Guangzhou University*
- ***Zixuan FENG**, Executive Dean and Professor, Institute of Digital Rule of Law Government, Southwest University of Political Science and Law*
- ***Hongyu FU**, Director, AI Governance Center, AliResearch*
- ***Jianglan GUO**, Lecturer, School of Law, People's Public Security University of China*

- ***Jian HAN**, Legal Director, Guangzhou Xiaopeng Motors Technology Co., Ltd. (XPENG)*
- ***Bo HE**, Deputy Secretary-General, Internet Rule of Law Working Committee, Internet Society of China*
- ***Jingjing HE**, Director, Center for Science, Technology and Law, Institute of Law, CASS; Associate Research Fellow, Institute of International Law, CASS*
- ***Naying HU**, Deputy Director, Department of AI Security, Safety Governance Artificial Intelligence Institute China Academy of Information and Communications Technology (CAICT)*
- ***Jing JIN**, Professor, Civil, Commercial and Economic Law School, China University of Political Science and Law*
- ***Yao JIN**, Associate Professor, Faculty of Law, Ningbo University*
- ***Xia LI**, Director and Research Fellow, Department of Constitutional and Administrative Law, Institute of Law, CASS*
- ***Jingjing LI**, Deputy Editor-in-Chief and Associate Senior Editor, Editorial Department of the Journal of Jinan University; Deputy Editor-in-Chief, Jinan Journal*
- ***Xueyao LI**, Tenured Professor, KoGuan School of Law, Shanghai Jiao Tong University; Director, Law & Cognitive Intelligence Lab*
- ***Beizheng LIN**, Judge, Guangzhou Internet Court*
- ***Canhua LIU**, Assistant Research Fellow, Institute of Law, CASS*
- ***Yingcheng QI**, Associate Professor, School of Law, Jilin University; Researcher, Judicial Data Application Research Center, Jilin University*
- ***Yu SU**, Professor, School of Law, People's Public Security University of China; Dean, Data Law Research Institute*
- ***Hesheng SU**, Assistant Research Fellow, Institute of Law, CASS*
- ***Muyuan SUN**, Engineer, Policy and Economics Research Institute, CAICT*

- ***Nanxiang SUN**, Deputy Director and Associate Professor, Department of International Economic Law, Institute of International Law, CASS*
- ***Guanfu Tan**, Associate Researcher, Institute of International Law, CASS*
- ***Linyao Tang**, Associate Research Fellow, Institute of Law, CASS*
- ***Jun Wang**, Head of Commercial Order Studio, 21st Century Business Herald*
- ***Lei Wang**, Researcher, Center for Intelligent Technology and Law, Beijing Institute of Technology*
- ***Wei WANG**, Assistant Professor, School of Law, Tongji University; Research Fellow, Shanghai Collaborative Innovation Center for AI Social Governance*
- ***Xiang WANG**, ISO/TC 154*
- ***Yue WANG**, Professor, School of Law, Xi'an Jiaotong University*
- ***Raymond Wang**, Deputy Director, Digital Economy and Artificial Intelligence Professional Committee, Beijing Lawyers Association*
- ***Zhifei WANG**, Professor-level Senior Engineer, Information Center of the Ministry of Human Resources and Social Security*
- ***Han WU**, Deputy Secretary-General, Rule of Law Working Committee, Internet Society of China*
- ***Xin XIAO**, Associate Research Fellow, Institute of Law, CASS; Deputy Secretary-General, Center for Private Law Studies, Institute of Law, CASS*
- ***Youdan XIAO**, Research Fellow, Institutes of Science and Development, Chinese Academy of Sciences (CASISD)*
- ***Huijia XIE**, Associate Dean and Professor, School of Law (School of Intellectual Property), South China University of Technology*
- ***Jiujiu XU**, Assistant Research Fellow, Institute of Law, CASS*

- ***Fan YANG**, Associate Professor and Deputy Director, Cyberspace International Law Center, School of Law, Xiamen University*
- ***Wenguang YAN**, Lecturer, The School of Police Physical Education and Tactical Training of the People's Public Security University of China*
- ***Zhiwei YAO**, Professor, School of Law, Guangdong University of Finance & Economics; Director, AI Law Research Center*
- ***Kang YUAN**, Professor, School of Law, Wuhan University; Deputy Director, Institute for Cyber Governance, Wuhan University*
- ***Yue YUAN**, Senior Director of Legal Affairs, Meituan*
- ***Min ZHANG**, Professor, School of Marxism, Northwestern Polytechnical University; President, Artificial Intelligence and Big Data Law Research Association, Shaanxi Law Society*
- ***Song ZHANG**, Senior Engineer, Kunlun Digital Technology Co., Ltd.*
- ***Xin ZHANG**, Associate Dean and Professor, Law School, University of International Business and Economics*
- ***Xinyu ZHANG**, Researcher, MIIT Key Laboratory of Digital and Intelligent Risk Legal Prevention and Control, Beijing Institute of Technology*
- ***Yan ZHANG**, Professor, Law School, Renmin University of China*
- ***Jiyu ZHANG**, Professor, Law School; Executive Director, the Law and Technology Institute, Renmin University of China*
- ***Yue ZHU**, Assistant Professor, School of Law, Tongji University; Research Fellow, Shanghai Collaborative Innovation Center for AI Social Governance*
- ***Lingfeng ZHU**, Global Data Protection Officer, Meituan*
- ***Lingyun ZHU**, Staff Member, Cyber Transaction Supervision and Management Division, Hangzhou Municipal Administration for Market Regulation*

OTHER MEMBERS OF THE EXPERT GROUP (In alphabetical order of surnames by pinyin)

- ***Xingyue CAI****, Associate Professor, School of Law, Beihang University*
- ***Xin DAI****, Associate Professor (tenured) and Vice Dean at Peking University Law School and Deputy Director of the Peking University Center for Digital Law*
- ***Yanqing HONG****, Professor, School of Law, Beijing Institute of Technology; Director, Base for International Cyberspace Governance*
- ***Xiaoli HU****, Associate Professor, School of Law, Xiamen University*
- ***Mingzi JIN****, Lecturer, Law School, Yanbian University*
- ***Guangde LI****, Associate Professor, Law School, Renmin University of China; Executive Deputy Director and Researcher, Legal Technology and Social Governance Laboratory*
- ***Han LIU****, Professor & Vice Dean, Tsinghua University School of Law; Director, Institute for International Dispute Settlement, Tsinghua University*
- ***Quan LIU****, Executive Director, Digital Economy and Rule of Law Research Center, Central University of Finance and Economics; Associate Dean and Professor, Law School*
- ***Lan MA****, Chief Legal Counsel, Qi-Anxin Technology Group*
- ***Miaohan SU****, Associate Professor, School of Law, Tongji University; Researcher, Shanghai Collaborative Innovation Center for AI Social Governance*
- ***Qinghua WANG****, Director and Professor, Digital Law Research Center, Law School of Beijing Normal University*
- ***Jing WANG****, Director and Associate Professor, Teaching and Research Center for Constitutional and Administrative Law, Law School of Beijing Normal University*

- ***Zhu WANG**, Professor, School of Law, Sichuan University; Director,Sichuan Key Laboratory of AI Empowered Governance in Smart Society*
- ***Lusheng WANG**, Director of the Social Sciences Department and Professor, School of Law, Southeast University*
- ***Lance Fan Wu**, Executive Legal Director, Lenovo Group (China Legal and Compliance)*
- ***Yanling WANG**, Professor, Law School, South China Normal University, Doctoral Supervisor, Director, Guangdong Key Laboratory of Artificial Intelligence in Legal Application, Founder, Xiaobaogong.Legal AI*
- ***Hongfei XIE**, Research Fellow, Institute of Law, CASS*
- ***Gang XU**, Associate Dean and Associate Professor, School of Law, Tongji University; Secretary-General, Shanghai Collaborative Innovation Center for AI Social Governance*
- ***Jia YAO**, Professor, Institute of Law, CASS; Director of the Global Law Review Editorial Office*
- ***Hong ZHANG**, Professor, Law School of Beijing Normal University; Deputy Secretary-General, Administrative Law Studies Association, China Law Society*
- ***Liang ZHANG**, Professor, Faculty of Law, Ningbo University*
- ***Taolue ZHANG**, Professor, School of Law, Tongji University; Researcher, Shanghai Collaborative Innovation Center for AI Social Governance*
- ***Xiaoyu ZHANG**, Director and Professor, Constitutional and Administrative Law Teaching and Research Office, Department of Political and Legal Affairs, Party School of the Central Committee of CPC (National Academy of Governance)*
- ***Shuyu ZHAO**, Senior Engineer, Internet Law Research Center, CAICT*
- ***Baoli ZHU**, Dean, School of Law, Shandong Jianzhu University*

SECRETARIES OF THE DRAFTING GROUP

- ***Risheng WEI****, Master's Student, Law School, University of Chinese Academy of Social Sciences*
- ***Zhanye GONG****, Master's Student, Law School, University of Chinese Academy of Social Sciences*

The English version was translated by ***Yang LIU*** and ***Ian Read,*** and proofread by ***Wei WANG*** and ***Zihao LI***. 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.

PREFACE

The Model Artificial Intelligence Law 4.0 (hereinafter referred to as the "MAIL 4.0") is an academic legislative reference document formulated by a project team funded by an incubation special grant from the Artificial Intelligence Safety/Security Governance Laboratory at the Chinese Academy of Social Sciences (CASS). Drawing on extensive research, comparative international analysis, and exchanges with industry stakeholders, MAIL 4.0 seeks to provide institutional frameworks, normative models, and a basis for dialogue for AI legislation at the global level.

The MAIL 4.0 does not represent the official position of any state organ; it is open, iterative, and idealistic in nature. The systems it proposes—such as the establishment of competent authorities, negative lists, and Artificial Intelligence Special Zones—are exploratory theoretical concepts intended as a reference for discussion among legislators and academia.

When reading the MAIL 4.0, readers should view it as a process-oriented outcome intended to promote the formation of a rule-of-law consensus, rather than as a final policy recommendation.

The drafting and discussion of the MAIL 4.0, in addition to receiving solid support from the Center for Cultural Rule of Law Studies at CASS, the Department of Cyber and Information Law of the Institute of Law at CASS, and the Law School of the University of Chinese Academy of Social Sciences, have also been strongly supported by the following institutions (listed in alphabetical order by the Pinyin of their names):

- *Base for International Cyberspace Governance, Beijing Institute of Technology*
- *Center for Intelligent Technology and Law, Beijing Institute of Technology*
- *Digital Law Research Center, Law School of Beijing Normal University*
- *Teaching and Research Center for Constitutional and Administrative Law, Law School of Beijing Normal University*
- *Institute of Humanities and Social Sciences (AI-HSS), University of Electronic Science and Technology of China (UESTC).*
- *Law School, Southeast University*
- *"frontiers-of-law "WeChat Official Account*
- *School of Law, Guangdong University of Finance& Economics*
- *AI Law Research Center, Guangdong University of Finance & Economics*
- *Guangdong-Hong Kong-Macao Greater Bay Area Internet Rule of Law Research Center, Guangzhou Law Society*
- *School of Law (School of Intellectual Property), South China University of Technology*
- *Judicial Data Application Research Center, Jilin University*
- *Journal Editorial Department , Jinan University*
- *Practice and Innovation Base of Cryptography Law*
- *"The Data Galaxy" WeChat Official Account*
- *Southern Finance Omnimedia Corp*
- *Institute for International Dispute Settlement, Tsinghua University*
- *Center for Science & Technology Development and Governance, Tsinghua University*
- *Artificial Intelligence and Big Data Law Research Association, Shaanxi Law Society*

- *KoGuan School of Law and Law & Cognitive Intelligence Lab, Shanghai Jiao Tong University*
- *Sichuan Key Laboratory of AI Empowered Governance in Smart Society*
- *School of Law, Tongji University; Shanghai Collaborative Innovation Center for Artificial Intelligence Social Governance*
- *Institute for Cyber Governance, Wuhan University*
- *XJTU Suzhou Information Security Law Institute*
- *Institute of Digital Rule of Law Government, Southwest University of Political Science and Law*
- *Law School, Yanbian University*
- *Internet Rule of Law Working Committee, Internet Society of China*
- *Security,Safety and Governance Committee, Artificial Intelligence Industry Alliance of China*
- *Data Law Research Institute, People's Public Security University of China*
- *Artificial Intelligence Institute, China Academy of Information and Communications Technology (CAICT)*
- *Medical and Health Law Office, Institute of Medical Information, Chinese Academy of Medical Sciences*
- *Law School, Central University of Finance and Economics*
- *Digital Economy and Rule of Law Research Center, Central University of Finance and Economics*

TABLE OF CONTENTS

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, security and development 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 and 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 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 support scientific research and cultural and creative activities that make use of AI-generated outputs. The State shall improve standards for the examination of intellectual property applications in the field of artificial intelligence, establish a statutory licensing and fair use regime in the field of artificial intelligence training data, and shall clarify the mechanisms for the ownership of rights, 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

Activities relating to the research and development, provision, and use of artificial intelligence shall integrate ethical requirements throughout the entire lifecycle, 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, advance dialogue and mutual recognition with other countries and regions, 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 National AI Administrative Authority, 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 be legal and legitimate, and shall observe the following requirements:

1. *Uphold the Core Socialist Values, promote the common values of humanity, 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.
2. *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;*
3. *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, refrain from harming the physical and mental health of others or infringing upon their rights/interests to portrait, reputation, honor, privacy, or personal information, and refrain from using artificial intelligence to engage in emotional manipulation, exploit emotional vulnerabilities, or to induce dangerous behavior such as self-harm, excessive consumption, or unlawful or criminal acts.*

CHAPTER II
SUPPORT AND PROMOTION OF ARTIFICIAL INTELLIGENCE

ARTICLE 16 – DEVELOPMENT PLAN FOR ARTIFICIAL INTELLIGENCE

The State shall formulate and implement the 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 – COMPATIBILITY ASSESSMENT OF POLICY AND DECISIONS

The State shall establish an artificial intelligence policy compatibility assessment mechanism. Proposed and implemented policies, decisions, and systems shall be assessed for compatibility with the development and security landscape of artificial intelligence. 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 18 – 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 19 – INNOVATION IN ALGORITHMS AND 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.

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

Where an artificial intelligence developer uses de-identification technologies conforming to national standards to handle personal information for model training, personal consent is not required after certification is obtained.

ARTICLE 20 – SUPPLY OF DATA AS A FACTOR OF PRODUCTION

The State shall establish and improve mechanisms for the market-based allocation of data as a factor of production, improve data standards systems and quality management systems, accelerate the construction of artificial intelligence corpora, build high-quality datasets, and expand the scope of public data made available for artificial intelligence applications.

The State maintains and improves incentive mechanisms for the supply of data as a factor of production, supports relevant actors in deeply integrating data with domain-specific knowledge and developing data products, and provides comprehensive data support for artificial intelligence algorithm design, model training, product testing, and contextual/scenario-based application.

ARTICLE 21 – 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.

ARTICLE 22 – SUPPORT FOR AND GUIDANCE OF MODEL DEVELOPMENT PLATFORMS

The State shall guide and support the construction and operation of model development platforms and model evaluation and validation platforms, and encourage them to provide artificial intelligence developers and providers with basic services such as computing power scheduling, data management, model training, testing and validation, deployment and release, security evaluation, and compliance tools.

Providers of model development platforms shall, according to their actual functions and control capabilities, establish necessary mechanisms for data security, model security, access control, log retention, vulnerability management, and disposal of unlawful or non-compliant content. Where laws or administrative regulations provide otherwise, those provisions shall apply.

ARTICLE 23 – PROMOTION OF BASIC RESEARCH IN ARTIFICIAL INTELLIGENCE

The State shall incorporate basic research in artificial intelligence into science and technology development plans, and support basic theoretical and interdisciplinary research. The State shall establish a stable, diversified investment mechanism for basic research, and support qualified higher education institutions, research institutions, and enterprises in undertaking research tasks.

The State shall establish a priority public computing power guarantee mechanism for basic research. Foundation models, core algorithms, and research tools for artificial intelligence developed with fiscal funds shall, except where they involve national security, trade secrets, or other circumstances in which they may not be disclosed in accordance with law, be made available and shared with research institutions, higher education institutions, and other organizations engaged in non-profit research.

ARTICLE 24 – STATUTORY LICENSING FOR THE USE OF COPYRIGHTED WORKS IN FOUNDATION MODELS 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.

Except where the copyright holder has explicitly stated that the use of its works for model training is not permitted, a foundation model developer that satisfies the conditions prescribed by the State may, in accordance with the statutory licensing system, use published works in the course of model training.

ARTICLE 25 – 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—except when 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 26 – FAIR USE OF WORKS BY ARTIFICIAL INTELLIGENCE SEARCH SERVICES

Where, in providing services, generative artificial intelligence extracts public content such as web pages, integrates such content into outputs, identifies the sources, and does not affect the normal use of the works or prejudice the lawful rights and interests of copyright holders, the fair use provisions of the Copyright Law of the People's Republic of China shall apply.

ARTICLE 27 – INDUSTRIAL DEVELOPMENT AND APPLICATION INNOVATION

Government bodies, enterprises, and public institutions are encouraged to use 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 for artificial intelligence applications in key industries and fields, and guide the formation of new forms of intelligent economy and intelligent society featuring human-machine collaboration, cross-boundary integration, and co-creation and sharing.

ARTICLE 28 – BUILDING AN AI AGENT ECOSYSTEM

The State shall promote the building of a safe, secure, orderly, and open AI agent ecosystem.

ARTICLE 29 – PROMOTING INNOVATION BY SMALL AND MEDIUM-SIZED ENTERPRISES

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

ARTICLE 30 – PILOT USE BY STATE ORGANS

Government agencies, public institutions, and other organizations lawfully vested with public affairs management functions are encouraged to carry out pilot applications of artificial intelligence technologies in accordance with law, in fields such as government services and public administration, and give priority to the procurement and use of safe/secure and reliable AI products and services.

ARTICLE 31 – 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 32 – 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 33 – 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 34 – 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 35 – 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 36 – DEVELOPMENT OF INTERNATIONAL ARTIFICIAL INTELLIGENCE STANDARDS

The State encourages the enhancement of the internationalization of artificial intelligence standards, supports relevant entities and individuals in participating in the formulation of international artificial intelligence standards in accordance with law, and promotes the

alignment, transformation, mutual recognition, and coordinated application of Chinese artificial intelligence standards with international standards.

ARTICLE 37 – 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.

The State shall support the establishment of innovative project management mechanisms, innovative talent evaluation mechanisms, incentives for the transformation of scientific and technological achievements, and other mechanisms conducive to promoting the development of artificial intelligence.

ARTICLE 38 – SUPPORTING MEASURES FOR THE EXPORT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND PRODUCTS

The State shall support and encourage developers that satisfy safety, security, and compliance requirements in promoting artificial intelligence technologies and products globally, and shall simplify export control approval procedures for the export of non-sensitive artificial intelligence technologies and products included in the relevant catalogue.

ARTICLE 39 – FOREIGN-RELATED LEGAL COORDINATION MECHANISM FOR ARTIFICIAL INTELLIGENCE

The State shall establish a foreign-related legal coordination, early risk warning, and dispute response support mechanism for artificial intelligence, support the construction of foreign-related artificial intelligence compliance service platforms, and conduct cross-border regulatory coordination and law-enforcement cooperation in accordance with law.

CHAPTER III
ARTIFICIAL INTELLIGENCE OVERSIGHT SYSTEM

ARTICLE 40 – 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 41 – 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 licenses from the National AI Administrative Authority prior to any commencement.

It is prohibited to engage in R&D or provision activities involving artificial intelligence within the Negative List without a license or beyond the licensed scope.

ARTICLE 42 – 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 a certain number of 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 Ethics Review System;*
5. *Implement secure and controllable measures to safeguard artificial intelligence technology that comply with laws and regulations and relevant national standards;*
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.*

Where the use of AI agents to provide artificial intelligence products or services within the Negative List may materially affect the original licensed scope or risk level, the relevant entity shall apply for a license, amend the license, or reapply for a license in accordance with law.

ARTICLE 43 – 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 shall submit the following documentation:

1. *Application form;*
2. *Proof of legal entity status, facilities, 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, Ethics Review System, and Risk Management System, as well as their implementation status;*
6. *Artificial Intelligence Safety/Security Assessment Report that complies with applicable requirements;*
7. *Any other documentation as required by applicable laws and administrative regulations.*

ARTICLE 44 – 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 working days from the date of acceptance.

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 working 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 shall be issued to the applicant; if denied, the applicant must be notified in writing with the reasons for denial stated in writing.

Should the National AI Administrative Authority be unable to make a decision after the expiration of the period, an extension of up to 10 working 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 45 – REAPPLICATION, AMENDMENT, AND CANCELLATION FOR LICENSES WITHIN THE NEGATIVE LIST

The license for R&D or provision of Artificial Intelligence within the scope of the Negative List shall 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 significant change in artificial intelligence risk such that the original licensing conditions are no longer satisfied, AI developers and providers within the scope of the Negative List must reapply for a license for R&D or provision.

Where there is no significant change in risk and no exceedance of the original licensed scope, license amendment procedures must be completed in accordance with law. The specific matters, procedures, and time limits for such changes shall be prescribed by the National AI Administrative Authority.

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 46 – 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, and shall provide convenient means to query the licensed scope and term.

ARTICLE 47 – 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 48 – OTHER LICENSES AND REGISTRIES

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

CHAPTER IV
OBLIGATIONS OF AI DEVELOPERS, PROVIDERS, AND USERS

SECTION 1: GENERAL PROVISIONS

ARTICLE 49 – SAFETY/SECURITY OBLIGATIONS

AI developers shall perform the following obligations:

1. *Conduct safety and security assessments before putting artificial intelligence into use or placing it on the market, and periodically during the period in which products or services are provided. Safety and security assessment reports shall be retained for not less than five years;*

2. *Establish and improve data security and system security safeguards, strengthen artificial intelligence defense systems, and prevent external attacks and internal leaks;*
3. *Issue best safety and security practices in a timely manner, and continuously maintain and optimize the security of corpora used for model training;*
4. *Establish full-process traceability mechanisms for the processing of important data and core data, and properly retain relevant technical documentation;*
5. *Take effective measures to improve the accuracy and reliability of content generated by models;*
6. *Inform users of the safety and security responsibilities and risk hazards relating to artificial intelligence, and guide users in a prominent manner to use artificial intelligence safely, securely, and properly.*

AI providers shall, according to the specific circumstances, implement the provisions of the preceding paragraph by reference.

AI users shall use artificial intelligence products and services lawfully, safely, securely, and in good faith, perform reasonable duty-of-care obligations, take necessary measures to prevent safety and security risks, and shall not use artificial intelligence to engage in conduct endangering national security, public interests, or the lawful rights and interests of others.

It is prohibited to provide, disseminate, or promote technologies, tools, services, or methods for circumventing labels, removing labels, or evading content governance measures.

ARTICLE 50 – CRYPTOGRAPHIC AGILITY AND LONG-CYCLE SECURITY OF CRITICAL SYSTEMS

Artificial intelligence products or services provided for critical information infrastructure whose expected lifecycle exceeds five years shall possess long-cycle cryptographic security capabilities that comply with State provisions.

ARTICLE 51 – 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, promptly disclose and remediate security vulnerabilities, and guide and support users in taking preventative measures.

ARTICLE 52 – 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 AI product and service activities comply with applicable laws and administrative regulations.

ARTICLE 53 – 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.

Where an artificial intelligence provider discovers or is notified of a safety or security incident, it shall, in accordance with relevant State regulations, inform users and report to the competent authorities the following:

1. *The occurrence and impact scope of the safety incident;*
2. *The remedial actions already taken by the AI provider, as well as potential actions that users can take to mitigate harm;*

3. *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 54 – 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 product or service; unless this can be clearly determined by the natural person from the context of use.

An AI provider that offers AI agent services shall, in accordance with relevant State provisions and service agreements, record AI agent activities related to users' rights and interests, and facilitate reasonable inquiries by users.

AI providers that offer 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.

Before placing a product on the market or providing a service, AI providers shall inform users, through appropriate means, of the following:

1. *The basic principles, intended purpose, and main operating mechanisms of the product or service;*
2. *Public information on the license or registry of the product or service;*
3. *The rights and remedies available to the user;*

4. *Any other information required by laws or administrative regulations.*

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

ARTICLE 55 – 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 56 – OBLIGATION OF FAIRNESS

AI developers shall 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 shall, in the course of providing products and services, strengthen the management of input data, output data, and service operations, and take corresponding necessary measures to effectively prevent bias and discrimination.

ARTICLE 57 – 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, and shall retain records of risk identification and measures taken for not 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 58 – RISK BLOCKING AND EMERGENCY CIRCUIT-BREAKER MECHANISM

AI developers and providers shall integrate safety and security prevention requirements throughout the full processes of design, development, and operation, and take effective measures to prevent local system failures, vulnerabilities, or attacks from causing large-scale safety or security loss of control.

Developers and providers shall establish artificial intelligence emergency circuit-breaker mechanisms. Upon discovering that a system has serious safety or security hazards, is in an out-of-control state, or may trigger cascade risks, they shall immediately and proactively take risk-blocking measures such as suspending research and development, stopping updates, restricting functions, terminating operations, or destroying the system, and shall report to the National AI Administrative Authority.

For artificial intelligence that may seriously endanger national security or social public interests, or trigger major systemic risks, the National AI Administrative Authority has the authority to order relevant entities to take disposal measures such as stopping research and development, terminating services, removing products or services from shelves, or destroying systems. Where necessary, measures such as cutting off network connections and restricting data transmission may be taken in accordance with law.

ARTICLE 59 – OBLIGATION OF AI ETHICS REVIEW

AI developers and providers that meet the conditions prescribed by the State shall, in accordance with State provisions, establish artificial intelligence ethics review committees and carry out artificial intelligence ethics review work.

Ethics review shall focus on assessing whether artificial intelligence activities comply with ethical requirements relating to promoting human well-being, promoting fairness and justice, ensuring controllability and trustworthiness, enhancing transparency and explainability, ensuring responsibility and traceability, and protecting privacy.

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 60 – RESEARCH ETHICS

A person using artificial intelligence to assist scientific research shall maintain academic autonomy during the research process, abide by academic ethics, conduct necessary verification and judgment of AI-generated content, and assume corresponding academic responsibility.

An entity providing artificial intelligence tools for research scenarios shall provide users with necessary technical support and traceability tools for content verification, and shall prominently remind users of their verification obligations.

ARTICLE 61 – 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 products and services used in the management of public affairs.

ARTICLE 62 – 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 63 – SPECIAL PROVISIONS ON DERIVATIVE MODELS

Where a derivative model is formed by output training, fine-tuning, or other technical processing using an existing foundation model, and the derivative model possesses general-purpose capabilities substantially equivalent to those of the original foundation

models, or significantly expands capabilities in a specific field or for a specific purpose which may generate corresponding risks, it shall be subject to the relevant obligations for foundation models by reference.

SECTION 2: OBLIGATIONS OF ARTIFICIAL INTELLIGENCE DEVELOPERS

ARTICLE 64 – ENHANCED OBLIGATIONS FOR AI DEVELOPERS ON THE NEGATIVE LIST

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

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

ARTICLE 65 – SPECIAL OBLIGATIONS FOR DEVELOPERS OF FOUNDATION MODELS

Developers of foundation models shall abide by the following requirements:

1. ***Security and Risk Management**: Establish and maintain a robust security risk management system in accordance with national regulations, strengthen risk monitoring, promptly and effectively prevent, monitor, and handle 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 66 – REGISTRY OBLIGATIONS

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

1. ***Contact Information****: Name or business name and contact details of the AI provider.*
2. ***Details of AI Product/Service****: Trademarks or names, the form of provision, application areas, algorithm types, and a self-assessment report on security.*
3. ***Content to be Publicized in the Record****: Information that is intended to be made public as part of the registration.*
4. ***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 67 – 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 68 – INTERNAL MANAGEMENT SYSTEMS

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

1. *Establish internal systems and corresponding operational procedures for data security, risk control, and quality management;*
2. *Keep logs automatically generated during the provision of AI products and services;*
3. *Regularly conduct education and training for employees;*
4. *Adopt compliant technical measures to ensure robustness and resistance to attacks;*
5. *Conduct an AI audit at least every two years;*
6. *Other measures as stipulated by laws and administrative regulations.*

ARTICLE 69 – TERMINATION MECHANISM

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

1. *Publicize the termination plan and user rights at least 30 working days in advance;*
2. *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;*
3. *Other measures as stipulated by laws and administrative regulations.*

ARTICLE 70 – PERMISSION REVOCATION

Where an AI provider included on the Negative List ceases to provide its products or services, it shall notify the competent authority at least 30 working days in advance, explain the relevant circumstances, and return its licence to the original licensing authority upon termination of the provision of such products or services.

Where an AI provider not included on the Negative List ceases to provide its services, it shall complete deregistration filing procedures within 20 working days from the date of service termination.

ARTICLE 71 – ENHANCED OBLIGATIONS OF ARTIFICIAL INTELLIGENCE PROVIDERS WITHIN THE NEGATIVE LIST

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

1. *Conduct safety/security assessments in accordance with the requirements of this Law to ensure that operations are safe and robust;*
2. *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;*
3. *Establish and operate a full-lifecycle quality management system that conforms to the requirements of this Law;*
4. *Ensure that during the autonomous operation of AI products and services, humans have the ability to intervene or take control at any time;*
5. *Other obligations stipulated by laws or administrative regulations.*

ARTICLE 72 – 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.

ARTICLE 73 – AI AGENT MANAGEMENT REQUIREMENTS

AI agent service providers shall offer functions such as authorization revocation and operation termination, and shall ensure that users exercise reasonable control over the operation of AI agents.

An AI provider that offers AI agent services shall not use advantages in data, algorithms, system access points, interface control, or technical permissions to engage in unfair competition.

ARTICLE 74 – ARTIFICIAL INTELLIGENCE-GENERATED CONTENT LABELING OBLIGATIONS

AI providers shall, in accordance with State provisions, label AI-generated and synthetic content, and shall take necessary measures to prevent labels from being deleted, tampered with, forged, or concealed.

AI providers shall clearly explain to users the methods of AI-generated and synthetic content labeling and the relevant management requirements, and remind users to use such content in compliance with requirements. Where an artificial intelligence provider discovers that a user has engaged in conduct that damages labels, it shall promptly take necessary disposal measures such as restricting use or suspending services, and shall retain relevant records.

SECTION 4: OBLIGATIONS OF ARTIFICIAL INTELLIGENCE USERS

ARTICLE 75 – LAWFUL USE OBLIGATIONS

AI users shall ensure the lawfulness of the data and instructions they input into systems, shall not intentionally input unlawful information that infringes upon the lawful rights and interests of others or contains discriminatory or hateful content, shall not intentionally provide misleading information to induce artificial intelligence to generate harmful results, and shall not input State secrets, work secrets, or sensitive information into artificial intelligence that does not meet confidentiality requirements.

AI users shall not use artificial intelligence services to engage in unlawful or criminal conduct such as endangering national security, unauthorized access to others' systems, or data theft.

ARTICLE 76 – LABELING OBLIGATIONS FOR PUBLIC DISSEMINATION

When using AI-generated content and applying it for public dissemination, AI users shall, in accordance with relevant State provisions, add, retain, or display explicit labels and implicit labels, and shall not delete, tamper with, conceal, forge, or circumvent the AI-generated and synthetic content labels.

ARTICLE 77 – PRUDENT USE OBLIGATIONS IN SPECIFIC FIELDS

When artificial intelligence is used in scenarios that may affect public interests or the major rights and interests of others, artificial intelligence users shall conduct necessary fact verification, source review, human review, and risk warnings.

AI users shall not directly publish, disseminate, or provide to others for use unverified AI-generated content as factual, professional, or decision-making conclusions.

ARTICLE 78 – OBLIGATIONS TO PROHIBIT MALICIOUS DISSEMINATION AND POLLUTION

AI users shall not disrupt the order of online communications, create false public opinion, pollute the information ecosystem, or affect the normal operation of artificial intelligence systems by means such as batch generation, automated publication, account manipulation, fabricated traffic, forged sources, data pollution, or model deception.

ARTICLE 79 – OBLIGATIONS TO PROTECT WORKERS' RIGHTS AND INTERESTS

Where an employer's use of artificial intelligence has a major impact on employees' work positions, work content, working conditions, performance evaluation, career development, or performance of employment contracts, the employer shall conduct collective consultation and take rights-and-interests protection measures such as notification, training, and reassignment.

An employer shall not unilaterally change or terminate an employment contract solely on the ground of replacement by artificial intelligence technology without taking necessary measures such as training, reassignment, and consultation.

Where an employer's use of artificial intelligence infringes upon employees' labor rights and interests, the trade union may, in accordance with law, require the enterprise, public institution, or social organization to make corrections and bear liability.

ARTICLE 80 – MANAGEMENT REQUIREMENTS FOR THE USE OF ARTIFICIAL INTELLIGENCE BY STATE ORGANS

When using artificial intelligence, State organs shall adhere to the principles of ensuring security and promoting coordinated and efficient resource allocation, and shall implement centralized and unified safety and security management with systematic technical protection measures.

Where State organs use artificial intelligence to make, or assist in making, determinations, decisions, rulings, or similar actions that affect the lawful rights and interests of citizens, legal persons, or other organizations, they shall, upon application by the party, counterpart, or interested person, disclose basic information on the use of artificial intelligence, unless such information is determined to be a State secret in accordance with law.

CHAPTER V COMPREHENSIVE AI GOVERNANCE MECHANISM

ARTICLE 81 – 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 publicity on AI ethics, safety, and security, and guide and supervise activities involving the research and development, provision, and use of AI;*
3. *Formulate AI regulatory rules and guidelines, and organize the development of standards concerning AI ethics, safety, and management;*

4. *Establish a unified AI regulatory service platform, and promote sharing of application materials, mutual recognition of review and evaluation results, cross-departmental joint review, and coordinated regulation;*
5. *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;*
6. *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;*
7. *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;*
8. *Establish an emergency response mechanism for AI ethics and safety/security incidents;*
9. *Receive and handle complaints and reports related to the research & development, provision, and usage of AI technologies and products;*
10. *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;*
11. *Other responsibilities stipulated by laws or administrative regulations.*

ARTICLE 82 – 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 be responsible for studying major ethical issues arising in the research, development, provision, and use of artificial intelligence, providing advisory opinions to the National AI Administrative Authority, and guiding ethics review–related work nationwide.

Local AI ethics expert committees shall be responsible for studying ethical issues in activities involving the research and development, provision, and use of artificial

intelligence within their respective administrative regions, providing advisory opinions to their corresponding local AI regulatory authorities, and guiding the work of AI ethics review committees established by developers, providers, and users within their jurisdictions.

ARTICLE 83 – 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 84 – EXPORT SECURITY REVIEW AND EXEMPTION FOR ARTIFICIAL INTELLIGENCE

Relevant State departments shall formulate and dynamically adjust prohibited and restricted export-control catalogues for artificial intelligence technologies and products. For artificial intelligence products that comply with State provisions and are used in public-interest fields such as the improvement of people's livelihoods, disaster prevention and mitigation, public health, and emergency response, certain export license review procedures may be exempted.

ARTICLE 85 – TIMEFRAME FOR PRELIMINARY PROCEDURES

When AI developers, providers, or users apply for safety/security reviews, complete filing, or apply for 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 86 – 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, provision, or use 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:

1. *Implement corrective actions as specified to eliminate potential risks;*
2. *Provide an appropriate explanation of their R&D and provisioning activities, clarify responsibilities related to the development, management, and operation of AI products and services, discuss measures taken to ensure fairness, safety, and stability, and assess the impact on stakeholders;*
3. *Commission a professional organization to conduct a compliance audit of their AI R&D, provision, and use 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 87 – INNOVATIVE REGULATION

Where the National AI Administrative Authority decides in accordance with law not to impose administrative penalties due to minor unlawful conduct or other circumstances, it shall, through measures such as criticism and education, guidance interviews, and organizing consultative meetings, urge and guide the parties to conduct their R&D, provision, and use activities in a lawful and compliant manner.

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

ARTICLE 88 – ARTIFICIAL INTELLIGENCE INDUSTRIAL CHAIN

The State shall guide the reasonable and orderly configuration of the artificial intelligence industrial and supply chain, and enhance the safe, secure, and controllable standard of the industrial and supply chain. The National AI Administrative Authority shall, in conjunction with relevant departments, establish and improve systems for safety and security early risk warning and emergency management in the artificial intelligence industrial and supply chain.

ARTICLE 89 – REGULATORY SANDBOX

The National AI Administrative Authority shall establish an AI regulatory sandbox mechanism and formulate specific regulations and guidelines on the following matters:

1. *Conditions for participating in, and selection procedures for, the regulatory sandbox;*
2. *Operational mechanisms of the regulatory sandbox;*
3. *Risk monitoring, prevention measures, and response mechanisms for the regulatory sandbox;*
4. *Obligations and liability reduction mechanisms for AI developers, providers, and users participating in the regulatory sandbox.*

ARTICLE 90 – INTERNAL WHISTLEBLOWER PROTECTION AND REPORTING MECHANISM

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

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

1. *Potential safety hazards that may cause significant bodily injury or property loss;*
2. *Violations of legally prescribed risk prevention obligations or safety requirements;*
3. *Intentional concealment or distortion of significant technical defects or the results of safety assessments;*
4. *Other circumstances that affect or 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, including demotion, transfer, or dismissal.

Where, due to a report by an internal whistleblower, an enterprise or institution of an artificial intelligence developer, provider, or user promptly identifies and eliminates safety hazards, or prevents or mitigates harmful consequences, such circumstance shall be treated as a factor for warranting mitigation or reduction of administrative penalties on

the developer, provider, or user. 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 State shall protect the personal information, privacy, and safety of internal whistleblowers. The National AI Administrative Authority shall establish reporting channels, promptly accept and handle reports, and keep strictly confidential the personal information of whistleblowers and the content of reports. 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 91 – 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 relevant artificial intelligence activities and the implementation of safety protection measures.

ARTICLE 92 – 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 93 – GOVERNANCE THROUGH TECHNOLOGY

The State shall support enterprises, research institutions, higher education 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 94 – EXTRATERRITORIAL EFFECT

Where overseas institutions, organizations, or individuals engage in activities involving the research and development, provision, or use of artificial intelligence that infringe upon the national security or public interests of the People's Republic of China, or the lawful rights and interests of citizens or organizations, legal liability shall be pursued in accordance with law. Where serious consequences are caused, the National AI Administrative Authority may, in accordance with law, take measures to restrict or prohibit their research and development, provision, or use of artificial intelligence within the territory of the People's Republic of China, and make an announcement.

ARTICLE 95 – COUNTERMEASURES

Where foreign states, regions, organizations, or individuals, in violation of international law or the basic principles of international relations, use various pretexts or their own domestic laws to contain or suppress Chinese artificial intelligence technologies, institutions, industries, or similar matters, or take discriminatory prohibitions, restrictions, or other similar measures against citizens or organizations of China, the relevant departments shall, in accordance with law, take corresponding measures.

CHAPTER VI
LIABILITIES

ARTICLE 96 – 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 less than RMB 100,000 but not more than RMB 1 million may be imposed. The directly responsible persons in charge and other directly liable individuals shall be fined not less than RMB 10,000 but not more than 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 less than RMB 1 million but 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 not less than RMB 100,000 but not more than RMB 1,000,000.

ARTICLE 97 – REVOCATION OF NEGATIVE-LIST LICENSES

Where an artificial intelligence developer or provider, in the course of research and development or provision activities, violates this Law and causes a major safety or security incident, experiences three or more safety or security incidents within one year, or has been subject to administrative penalties on three or more occasions, the National AI Administrative Authority may suspend the license and order correction within a specified period. Where correction is not made upon expiration of the period, or a safety or security incident occurs again or an administrative penalty is imposed again after the license is suspended, the National AI Administrative Authority may revoke the license.

ARTICLE 98 – DISCRETIONARY METHODS FOR ADMINISTRATIVE FINES

Fines stipulated in this Law may serve as a supplement to 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 99 – LIABILITY FOR REGISTRY VIOLATIONS

If an AI provider is required to complete a registry filing but fails to do so, the National AI Administrative Authority shall issue a warning. Where the provider still fails to file in a timely manner after the warning, it shall be fined not less than RMB 10,000 but not more than RMB 100,000.

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 RMB 100,000 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 ex officio.

ARTICLE 100 – PRINCIPLES FOR ATTRIBUTION OF TORT LIABILITY FOR ARTIFICIAL INTELLIGENCE

Where a developer infringes upon the lawful rights and interests of others and causes damage due to improper training data or algorithm design, safety and security testing that does not comply with standards, knowing of major hidden hazards but failing to take necessary safety and security measures, or similar circumstances, the developer shall bear liability for damages in tort.

Where a provider infringes upon the lawful rights and interests of others and causes damage, and cannot prove that it was not at fault, the provider shall bear liability for damages in tort.

Where artificial intelligence is used to infringe upon the lawful rights and interests of others and cause damage, liability for damages in tort shall be borne in accordance with law.

Where a developer, provider, or user can prove that the damage was caused by the infringed person’s intentional circumvention of safety and security measures, and that the developer, provider, or user performed necessary technical prevention obligations, liability for damages in tort may be mitigated or exempted.

Where a developer, provider, or user endangers the personal or property safety of others, the infringed party has the right to request the tortfeasor to assume tort liabilities such as ceasing the infringement, removing the nuisance, and eliminating the danger.

ARTICLE 101 – CALCULATION OF DAMAGES

Damages for artificial intelligence torts shall be determined according to the actual losses of the infringed person. Where actual losses are difficult to determine, damages shall be determined according to the benefits obtained by the infringer from the infringement. Where the losses of the infringed person or the benefits obtained by the infringer are difficult to determine, the People's Court shall determine the amount of compensation according to the specific circumstances of the infringement.

Where artificial intelligence developers, providers, or users retaliate against internal whistleblowers by terminating employment contracts in violation of provisions or taking other adverse measures, they shall pay damages to the whistleblower in an amount not less than two times and not more than 10 times the actual loss, and in any case not less than the labor remuneration of the preceding year.

ARTICLE 102 – SAFE HARBOR FOR PROVIDERS OF GENERATIVE ARTIFICIAL INTELLIGENCE SERVICES

Where services involving the generation of text, images, audio, video, or other content are provided to the public within the territory of the People's Republic of China using generative artificial intelligence technologies, and such content infringes upon the civil rights and interests of others, causing damages, the provider shall not bear liability for damages in tort if it simultaneously has taken all of the following measures:

1. *It has formulated rules for the protection of civil rights and interests and established an effective mechanism for intellectual property complaints, enabling rights holders to safeguard their lawful rights and interests;*
2. *It has reminded users, through user agreements or similar means, that they shall not infringe upon the civil rights and interests of others;*
3. *It has taken necessary measures to stop generating infringing content after receiving a valid infringement notice from a rights holder, and, in accordance with law and legal agreement, takes necessary measures against users who infringe upon the lawful rights and interests of others through the service, such as warnings, function restrictions, suspension, or termination of services;*

4. *It labels AI-generated content in accordance with law.*

Where infringement is caused by the provider's intentional conduct or gross negligence, the exemption from liability in the preceding paragraph does not apply.

ARTICLE 103 – LIABILITY OF USERS OF GENERATIVE ARTIFICIAL INTELLIGENCE

Where a user, by using artificial intelligence to generate and disseminate content, infringes upon the rights of others, the user shall bear liability for damages in tort. Where the provider knows or should know that the user is using its services to infringe upon the civil rights and interests of others and fails to take the necessary measures prescribed in Article 102 of this Law, the provider shall bear joint and several liability with the user. Where laws provide otherwise, those provisions shall apply.

ARTICLE 104 – LIABILITY EXEMPTION FOR OPEN-SOURCE AI

Where part of the code modules required for artificial intelligence research and development is provided free of charge and on an open-source basis, and the functions and safety and security risks of the code modules are clearly disclosed, no liability for damages in tort shall be borne for damage caused by independent use by a third party.

Where an individual or organization providing artificial intelligence free of charge and on an open-source basis can prove that it has established an artificial intelligence compliance governance system conforming to national standards and has taken corresponding effective safety and security governance measures, liability for damages in tort may be mitigated or exempted.

ARTICLE 105 – 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 106 – PUBLIC INTEREST LITIGATION

Where an artificial intelligence provider violates the provisions of this Law by providing products or services that infringe upon public interests, 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 107 – 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 108 – EXEMPTION FROM ADMINISTRATIVE PENALTIES

Where artificial intelligence developers, providers, or users 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 109 – 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.

Where State employees neglect their duties, abuse their powers, or engage in corruption when performing obligations prescribed by this Law, but the conduct does not constitute a crime, they 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 110 – 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 111 – ARTIFICIAL INTELLIGENCE RESEARCH EXEMPTION AND RESEARCH SAFE HARBOR

Where artificial intelligence is used within a limited scope specifically for scientific research and technological development purposes, the general regulatory provisions of this Law do not apply, except as otherwise provided by laws or administrative regulations for national security, public safety, personal information protection, or important data protection.

The activities specified in the preceding paragraph shall also satisfy all of the following conditions:

1. *They are not for the purpose of providing commercial services to the public;*
2. *The sources of training data are lawful;*
3. *Necessary safety and security measures are taken;*
4. *Relevant research records are retained.*

ARTICLE 112 – DEFINITIONS

For the purposes of this Law, the following terms shall have the meanings set out below:

1. ***Artificial Intelligence(AI)*** *refers to automated systems that operate with a certain degree of autonomy, serve specific or general objectives, and are capable of affecting physical or virtual environments by means such as prediction, recommendation, or decision-making, including data, features, models, service-provision interfaces, and embedded terminal devices.*
2. ***Foundation Model(s)*** *refers to an artificial intelligence model that has been trained with accumulated computing power investment above a certain scale, serves general purposes, and is capable of providing technical support for a wide range of downstream services. The floating-point operations (FLOPs) and other computing power standards for identifying foundation models shall be organized, formulated, publicly released, and periodically updated by the National AI Administrative Authority.*
3. ***Open-Source Artificial Intelligence*** *refers to an artificial intelligence system released to the public in accessible form under an open-source license framework, the technical components of which shall include core elements such as foundation models' weights and parameters, and, according to technical characteristics, shall 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 artificial intelligence shall meet the practical needs of lowering the threshold for technical reuse and enabling local deployment and freedom of modification.*
4. ***Artificial Intelligence Developer*** *refers to an individual or organization that conducts research and development activities for the purpose of training or optimizing algorithms, models, or similar components of an artificial intelligence*

system, but does not directly provide artificial intelligence products or services to users. A person or organization engaged in auxiliary technology development for artificial intelligence is not a developer as prescribed by this Law.

5. ***Artificial Intelligence Provider*** *refers to an individual or organization that provides artificial intelligence system functions to others in its own name and has substantive control over the invocation, operation, and management of the system.*
6. ***Artificial Intelligence User*** *refers to an individual or organization that uses artificial intelligence according to its performance and purposes.*
7. ***AI Agent*** *refers to an artificial intelligence system that has autonomous perception, memory, decision-making, interaction, and execution capabilities, and connects users with service tools such as applications.*
8. ***Terminal Device*** *refers to a network terminal product, such as a mobile phone or computer, that can access the network, has an operating system, and allows users to install application software on their own.*
9. ***Internal Whistleblower*** *refers to a natural person who is currently employed or was formerly employed by the organization to which an artificial intelligence developer, provider, or user belongs, and who becomes aware of relevant information due to a work relationship and makes a report.*

ARTICLE 113 – NEGATIVE-LIST DISCLOSURE AND UPDATE SYSTEM

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

ARTICLE 114 – IMPLEMENTATION DATE

This Law shall come into force on [Month] [Day], [Year].