2026

Chery Artificial Intelligence Compliance White Paper

Message

Today, a Chery vehicle can understand local accents, anticipate a curve ahead, park itself neatly into a space, and even suggest a break when it senses driver fatigue, and we know what truly powers these capabilities. It is not parameters and computing power alone—but a genuine understanding of people, a reverence for life, and a conscious commitment to responsibilities.

Artificial intelligence is weaving itself into every moment of mobility with unprecedented depth. It gives machines the ability to perceive and to think, while also bringing new questions: How do we clear the first and most critical threshold—proving safety where lives are at stake? How do we build an AI governance framework aligned with human values? How do we ensure AI systems remain stable, reliable, and traceable across their entire lifecycle? These are no longer technical footnotes; they are foundational issues tied to users' safety, dignity, and well-being.

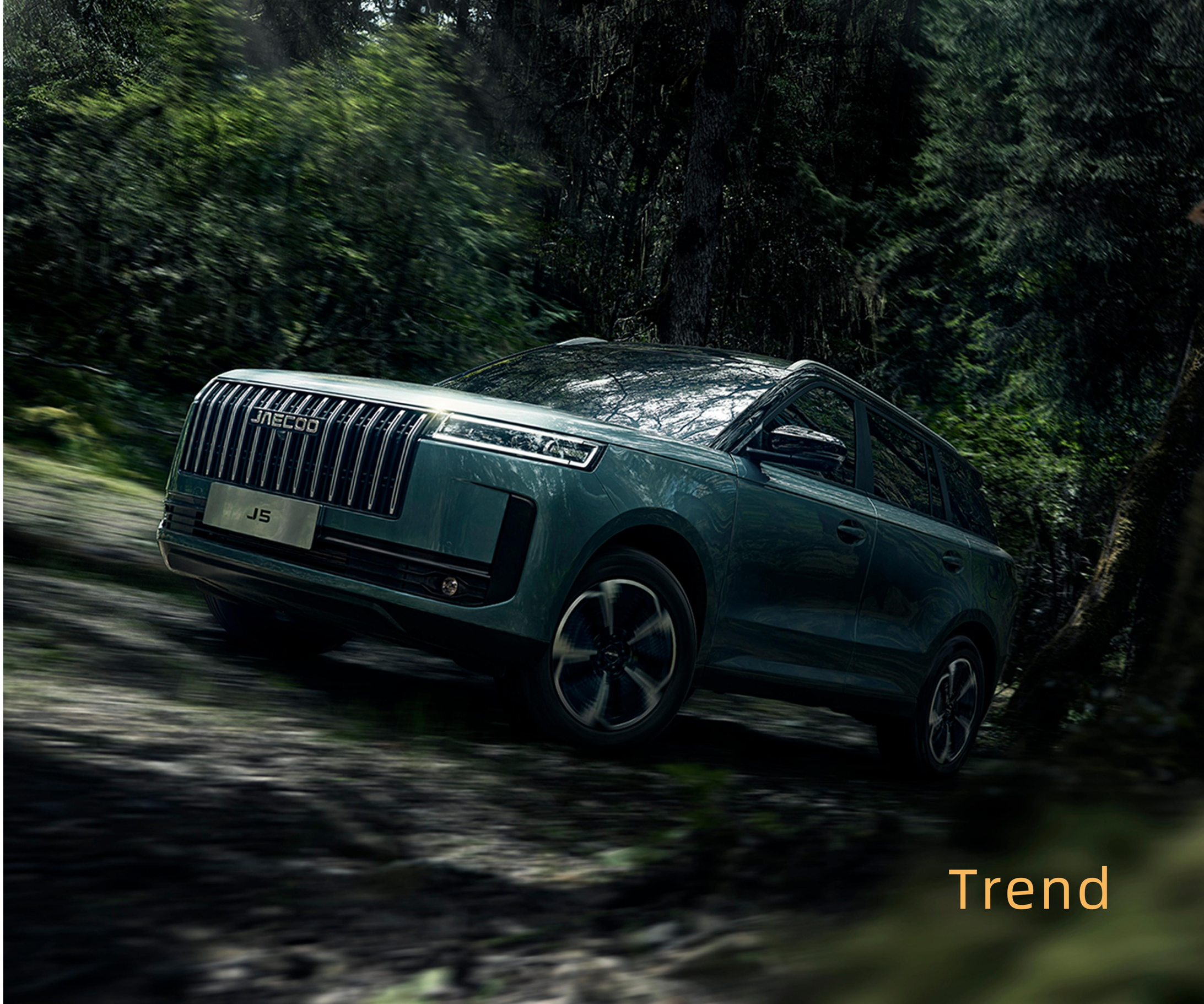
In the face of the rapid technological evolution and profound shifts in the global regulatory landscape, Chery has always held "people first" as the defining principle of intelligent innovation. We remain clear-eyed: AI is a powerful and captivating tool. It must serve humanity faithfully—and never become a runaway force beyond control. That is why we are actively building a future-oriented governance and compliance framework for AI. We are working to embed algorithmic transparency, information security, privacy protection and ethical considerations into our R&D, products, and services, so as to align with regulatory expectations at home and abroad while advancing a higher standard for trustworthy AI in mobility.

At Chery, we believe AI must advance not only toward what is new, but also toward what is good. Let technology benefit everyone; let industry grow more prosperous; let the society of tomorrow be richer, fairer, and warmer—this is the ultimate meaning of AI, and it is Chery's unwavering original intent.

It is in this spirit that this white paper has taken shape. It reflects our observation of global regulatory trends, our learning from leading industry practices, and our reflection on our path to compliance. It is a commitment Chery makes—to our users, to the community, and to the future.

Chairman of the Board Chery Automobile Co., Ltd.

CONTENT



Trend

CHERY 2026
DATA COMPLIANCE

AI Enters the Era of Institutionalized Regulation

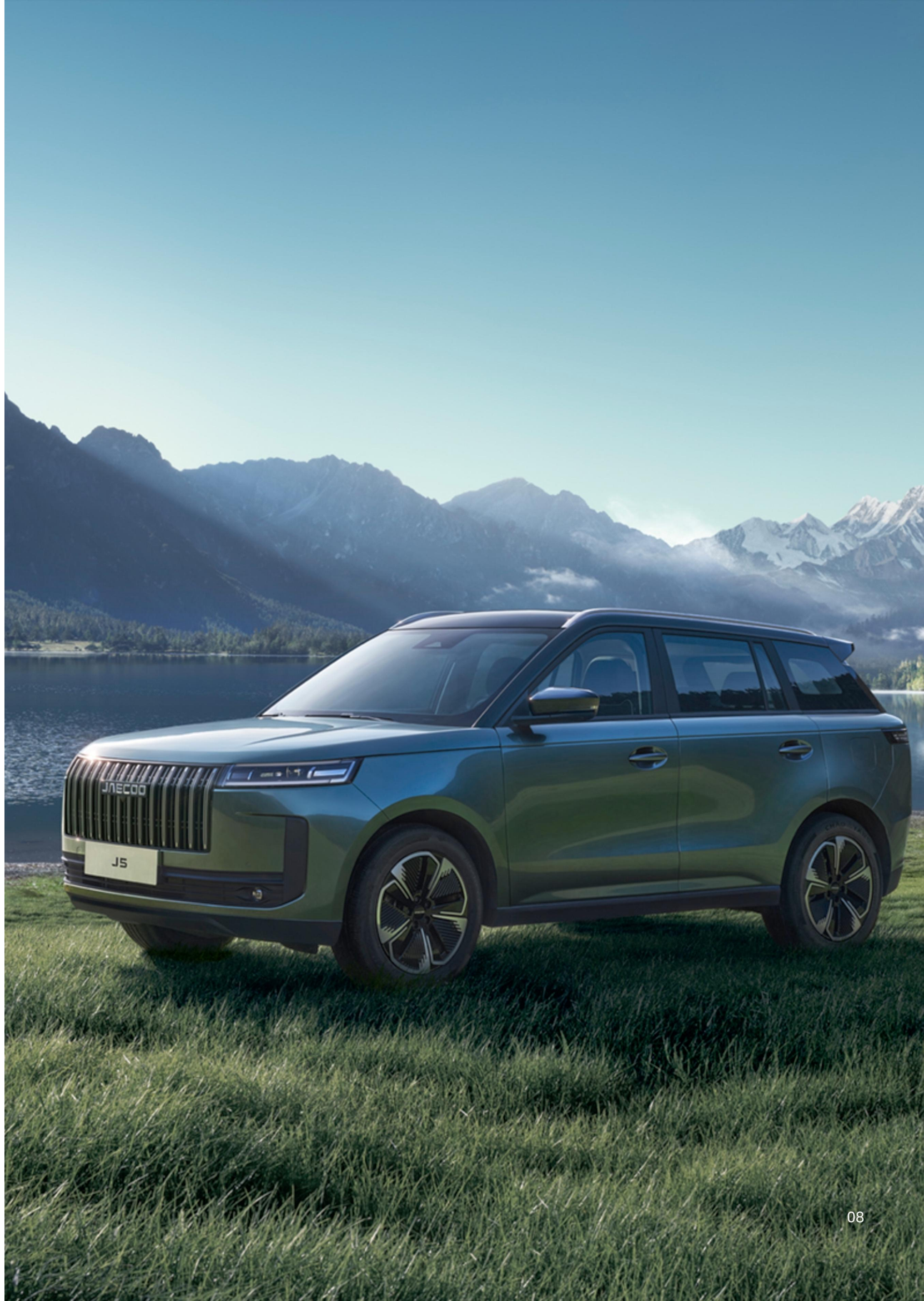
I. AI as a Next-Generation Strategic Technology

In 1956, Artificial Intelligence (AI) was formally proposed as a field of research, marking the start of efforts to achieve machine intelligence through computational methods. Over the subsequent decades, AI has progressed through multiple technical approaches, from rule- and knowledge-driven to data-driven, and has experienced successive waves of technological innovation and downturns.

Since 2010, deep neural networks achieved pivotal breakthroughs, supported by large-scale data and computing power. Rapid advances in capabilities such as image recognition and speech processing also enabled the large-scale application of AI.

Following the introduction of the Transformer architecture in 2017, large-scale pre-trained models entered a phase of rapid development. In the course of scaling, the phenomenon of "emergence" occurred, that is, unexpected new capabilities surfaced once model scale surpassed a critical threshold. Since 2022, generative AI, represented by ChatGPT, has rapidly proliferated through conversational interactions. More recently, the development of multimodal capabilities and the trend toward agentic AI have further driven the broader adoption of AI applications.

As AI capabilities advance, risks arising from AI applications continue to grow, and numerous challenges, from data infringement and algorithmic bias to system security and reliability, are becoming increasingly evident. Inevitably, AI governance and compliance become a core issue on par with technological innovation and must be taken care of in parallel.



AI Enters the Era of Institutionalized Regulation

II. Common Risks of AI Applications

The risks of AI applications span the entire lifecycle. Taking AI systems regulated by numerous countries as a typical example, we have summarized the following categories of common risks:

1. Data Infringement: The training of AI systems is highly dependent on data inputs. The unlawful collection, processing, and use of training data may result in unlawful processing of personal data or infringement of intellectual property rights.

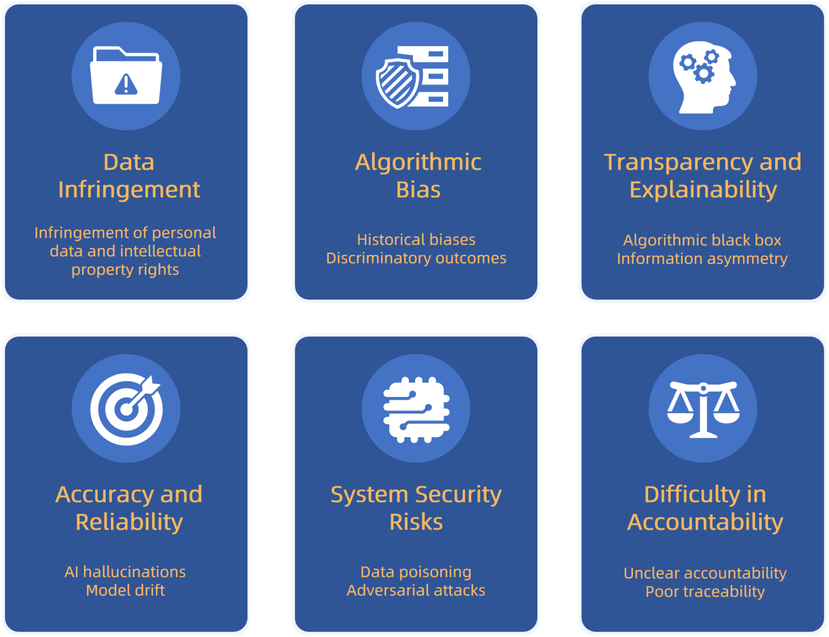
2. Algorithmic Bias: AI systems may absorb and inherit historical biases present in training data, leading to unfair or discriminatory decision-making that affects individual rights and interests (typical scenarios include recruitment, credit, and marketing), and even undermining the legitimate rights and interests of specific groups and social equity.

3. Transparency and Explainability: Some AI systems possess "black-box" attributes. When coupled with insufficient information disclosure by service providers, this can easily create information asymmetry. Users may be unable to identify the interaction counterparty, may fail to understand the decision-making logic, or may find it difficult to discern the authenticity of content, resulting in restricted rights to know and autonomous choice and potential exposure to misleading or false information.

4. Accuracy and Reliability: AI systems typically operate based on probabilistic prediction mechanisms and may produce "hallucinations"—for example, generating untrue or fabricated content—or experience "model drift" in long-tail scenarios, leading to performance degradation. In low-fault tolerance fields such as transportation and healthcare, any deviation in outputs may cause bodily injury or major property loss.

5. System Security Risks: The input sensitivity and data dependency of AI systems may be exploited by malicious third parties. For example, a third party may create system misjudgment through "adversarial attacks", or tamper with the model's intended behavior through "data poisoning", thereby leading to loss of system control, leakage of key business information, failure of security defenses, and other consequences.

6. Difficulty in Accountability: The automated decision-making, "black-box" attributes, and continuous post-launch iterations of AI systems make it difficult to effectively clarify the causal chain between human intent, system decisions, and harmful consequences. In the absence of traceability mechanisms (such as log records and retention of key files) covering the entire lifecycle, it may be difficult to audit or effectively attribute liability after damage occurs because of insufficient evidence or an irreproducible decision-making process.



AI Enters the Era of Institutionalized Regulation

III. Evolution of AI Governance

National governments and international organizations have long been attentive to the potential risks of AI applications. Over the past decade, AI governance has evolved globally from ethical codes toward institutionalized regulation:

1. Ethical Codes Stage (Mid-to-Late 2010s)

In the mid-to-late 2010s, while machine learning achieved breakthroughs, societal concern regarding the risks of AI applications also increased. Several national governments and international organizations—including the Organization for Economic Co-operation and Development (OECD) and the European Union (EU)—successively issued a series of AI ethical codes intended to provide standards-based guidance for the development and application of AI. By articulating values-based and behavioral principles, such as advocating a people-centered approach and respect for human rights, emphasizing fairness and non-discrimination, and requiring transparency and explainability, these principles provided a framework to create subsequent policymaking on AI and to encourage corporate self-governance.

However, the limitations of ethical codes also became apparent: high-level principles are difficult to turn directly into actionable, specific requirements, and profit motives inherently render exclusive reliance on corporate self-regulation inadequate for mitigating system risks. This understanding has been progressively reflected in key policy papers; for example, the White Paper on Artificial Intelligence (2020) issued by the EU and the Recommendation on the Ethics of Artificial Intelligence (2021) issued by UNESCO have explicitly advocated regulatory policies to enhance the practice of ethical codes.

2. Institutionalized Regulation Stage (Since 2020)

Since 2020, AI governance has entered a new stage of institutionalized regulation. According to the OECD.AI Policy Navigator, as of February 2026, more than 80 jurisdictions and international organizations worldwide have promulgated 2,214 AI-related policies and regulatory initiatives. Currently, an evolving global regulatory landscape that covers the AI application lifecycle and focuses on risk governance begins to take shape.

The following chapter will conduct a systematic scan of the global AI regulatory landscape from two perspectives: macro trends and specific regulations, presenting our observations on regulatory approaches across different jurisdictions, and analyzing the core requirements of typical global AI regulatory rules.

Observation

The Global AI Regulatory Landscape

I. Macro Observations on Global AI Regulatory Trends

Feature 1: Major jurisdictions exhibit a dual dynamic of "dense rollout of rules" and "de-regulatory reflection".

- **Dense Rollout of Rules:** Between 2022 and 2023, China adopted an "incremental, fast-paced approach" and successively promulgated specific regulations governing algorithm recommendation, deep synthesis, and generative AI. In 2024, the EU Artificial Intelligence Act officially took effect; subsequently, South Korea passed the Basic Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness. The United States, the United Kingdom, Brazil, and other countries and regions have also continued to advance the drafting and discussion of AI-related laws and policies.
- **De-regulatory Reflection:** As regulatory rules are introduced worldwide at a rapid pace, some jurisdictions are also reflecting on the challenges of over-regulation and seeking a new balance between risk control and technological innovation. As a pioneer in AI regulation, the EU has shown signs of adjustment during the implementation of its Artificial Intelligence Act. In November 2025, the European Commission released the Digital Omnibus Package, proposing to simplify and defer certain obligations and implementation timelines to ease compliance burdens. Australia, Canada, and other governments have also emphasized the chilling effect of excessive regulation on innovation; the United States has advanced de-regulatory reforms for AI development through executive orders. However, these adjustments have not altered the overall trend of continuous advancement in global AI regulation.

Feature 2: Major jurisdictions show convergence in regulatory approaches, governance scope, and core regulatory elements.

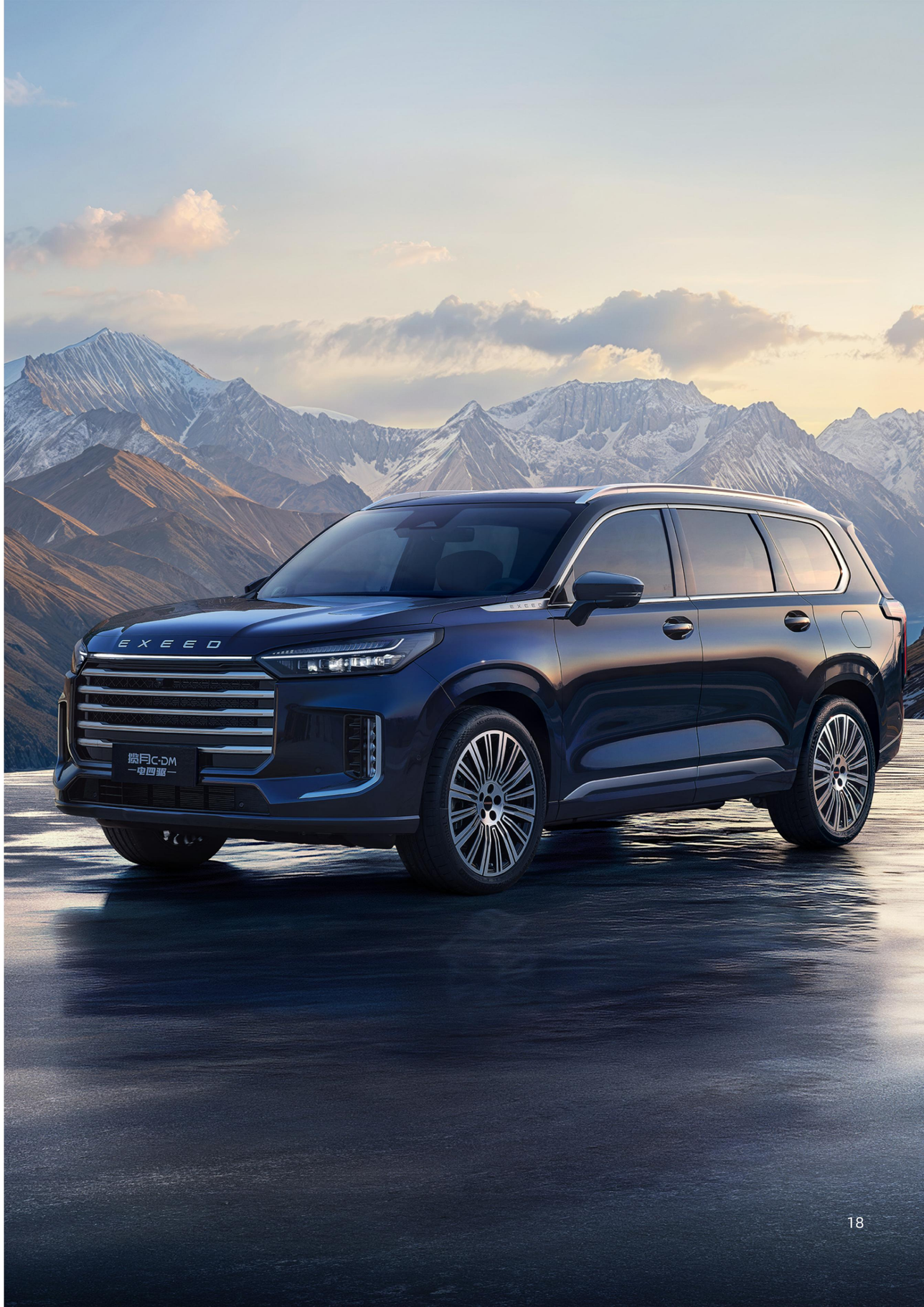
- **Risk-oriented Approach:** The level of regulatory intervention and the regulatory design are determined based on the risk level of AI systems or application scenarios. For instance, jurisdictions such as the EU and South Korea focus on "high-risk" or "high-impact" AI systems and generative AI; China prioritizes specific AI technical forms such as algorithm recommendation, deep synthesis, and generative AI.
- **Full Lifecycle Governance:** Emphasis is placed on the full lifecycle of AI systems, including design, development, deployment, and operation, requiring continuous identification, assessment, management and control of risks at each stage.
- **Convergence of Core Regulatory Elements:** Common regulatory elements focus on implementing data governance requirements, ensuring system reliability and security, strengthening information disclosure and transparency, improving the organizational governance and risk management mechanisms, protecting user rights and other key aspects.

The Global AI Regulatory Landscape

Feature 3: Major jurisdictions' regulatory tools and legislative structures continue to diverge.

- **Coexistence of Hard Law Constraints and Soft Law Guidance:** Jurisdictions such as the EU, China, and South Korea have established regulatory baselines through binding legislation or administrative regulations ("Hard Law"), defining obligations and penalties. Meanwhile, jurisdictions such as the UK, Singapore, and Australia primarily rely on principle-based guidance, industry guidelines, and voluntary frameworks ("Soft Law") to promote organizational self-governance.
- **Divergent Evolution of Horizontal Unified Regulation and Vertical Segmented Regulation:** Jurisdictions such as the EU and Brazil establish a unified horizontal regulatory framework through comprehensive AI legislation ("Horizontal Unified Regulation"). On the other hand, the UK and Australia rely on dispersed governance through existing sectoral regulations, while China implements vertical specific regulation targeting technical modalities such as algorithm recommendation, deep synthesis, and generative AI ("Vertical Segmented Regulation").

Notably, these divergences are better understood as transitional differences in regulatory approaches rather than their ultimate form. Most jurisdictions continue to adjust their regulatory tools and legislative structures, and there remains room for mutual learning and transformation in both hard-law/soft-law and horizontal/vertical regulatory approaches. The global AI regulatory framework remains in continuous evolution.



The Global AI Regulatory Landscape

II. Panoramic Overview of Global AI Regulatory Requirements

In the following sections, we conduct a systematic review of AI regulatory policies in major global economies, focusing on AI-specific rules that have been formally issued or have entered substantive legislative processes and are applicable to enterprises, including both Hard Law and broadly influential Soft Law.Based on the review, we have compiled an Overview Table of global AI regulatory requirements to clearly present the characteristics of AI governance across major jurisdictions.

Jurisdiction[1]		General Regulatory Requirements																			
		Documents Name	Legal Effect	Scope of Application[2]	Data Governance		System Accuracy, Reliability and Cybersecurity		Transparency and Information Disclosure Requirements							Organizational Governance and Risk Management					User Rights		Prohibitions
					Lawful Data Sourcing	Data Quality Assurance	Accuracy and Reliability	Cybersecurity	Prior Notification	Explanation of Decisions	Content Labeling	Public Disclosure	Downstream Information Provision	Regulatory Filing	Incident Reporting	Governance Framework	Conducting Assessments	Human Oversight	Traceability	AI Literacy	Right to Appeal	Right to Non-discrimination	Explicitly Prohibited Matters
China		Provisions for the Administration of Algorithmic	✓	Recommendation Algorithm	○	○	●	●	●	●	●	●	○	●	●	●	●	○	●	○	●	●	●
		Provisions on the Administration of Deep Synthesis of Internet-based Information Services	✓	Deep Synthesis	●	○	●	●	○	○	●	●	○	●	●	●	●	○	●	○	●	○	●
		Interim Measures for the Administration of Generative Artificial Intelligence Services	✓	AIGC	●	●	●	●	○	○	●	●	○	●	●	○	●	○	●	●	●	●	●
European Union		Artificial Intelligence Act	✓	AI System	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	○	●	●
United States	California	Generative Artificial Intelligence: Training Data Transparency	✓	AIGC	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○
		AI Transparency Act	✓	AIGC	○	○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
	New York	Responsible AI Safety and Education Act	✓	AI System	○	○	○	●	○	○	○	●	○	●	●	●	●	○	●	○	○	○	●
	Colorado	Consumer Protections for Artificial Intelligence	✓	High-Risk AI System	○	●	○	○	●	●	○	●	●	○	●	●	●	○	●	○	●	●	○
South Korea		Basic Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness	✓	High-Impact AI System	○	○	●	●	●	●	●	○	○	○	○	●	●	●	●	○	○	○	○
Vietnam		Law on Artificial Intelligence	✓	AI System	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	○	○	●	●
Kazakhstan		On Artificial Intelligence	✓	AI System	●	●	●	●	●	●	●	○	○	○	○	●	●	○	●	○	●	●	●
El Salvador		Law For The Promotion Of Artificial Intelligence And Technologies	✓	AI System	●	○	○	○	●	●	○	○	○	○	○	○	○	○	○	○	●	●	○
Turkey		Artificial Intelligence Law Bill	⊖	AI System	●	○	●	○	○	○	○	●	○	●	○	●	●	○	○	○	○	●	●
Brazil		Bill on the use of Artificial Intelligence	⊖	AI System	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●
Argentina		Legal regime for the responsible use of AI	⊖	AI System	●	●	●	●	●	○	●	●	○	●	●	●	●	○	●	●	○	●	●
Canada		Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems	◎	AIGC	●	●	●	●	○	○	●	●	●	○	○	●	●	●	●	●	○	●	○
Australia		Guidance for AI Adoption: Implementation practices	◎	AI System	●	○	●	●	●	●	●	○	●	○	●	●	●	●	●	●	●	●	○
Japan		Act on Promotion of Research and Development, and Utilization of Artificial Intelligence-related Technology and Its Applicable Guidelines	◎	AI System	●	○	●	●	○	●	●	●	○	○	○	●	●	○	○	●	○	●	○
Singapore		Model AI Governance Framework for Generative AI	◎	AIGC	●	●	●	●	○	○	●	○	●	○	●	○	●	○	○	●	○	●	○
Hong Kong		Generative Artificial Intelligence Technical and Application Guideline	◎	AIGC	●	●	●	●	○	○	●	●	●	○	○	●	●	●	●	○	○	●	●

[1] Geographic Scope: In addition to the jurisdictions listed in the Overview Table, we have also examined the AI regulatory status in 19 other jurisdictions, including Switzerland, and India. However, these jurisdictions are not included in the Overview Table because they have not yet enacted formal AI legislation, their legislative processes remain subject to significant uncertainty, and they lack widely binding normative instruments.

[2] Scope of Application: The AI systems referenced in the Overview Table encompass AI systems, models, products, and services. Most regulatory requirements listed in the table apply only to specific categories of AI systems—such as high-risk AI systems, high-impact AI, or generative AI—rather than to all AI systems. For specific details, please refer to the relevant provisions in each jurisdiction's normative documents.

Legend: ⊖ Under Legislative Process (Hard Law) ✓ Adopted / Effective (Hard Law) ◎ Adopted (Soft Law)

The Global AI Regulatory Landscape

We have categorized the regulatory requirements covered in the Overview Table into six core modules: Data Governance, System Accuracy, Reliability and Cybersecurity, Transparency, Organizational Governance and Risk Management, and User Rights and Prohibitive Requirements.

1. Data Governance

Data governance is the core requirement to control AI data risks. Key focuses include:

- Lawful Data Sourcing: Requires that the acquisition and use of data for training, validation, and testing of AI systems possess a legal basis and comply with personal data protection laws and intellectual property laws.

EXAMPLE: Under Articles 10 and 53 of the EU AI Act, training, validation, and testing data for high-risk AI systems shall be subject to data governance and management practices, particularly regarding data origin and, for personal data, its original collection purpose. Providers of general-purpose AI models must also adopt policies to comply with EU copyright rules.

- Data Quality Assurance: Requires training, validation, and testing data to be relevant, representative, as complete and error-free as possible, and to enable the identification and mitigation of biases that may lead to discriminatory results.

EXAMPLE: Article 7 of the Interim Measures for the Administration of Generative Artificial Intelligence Services (China) stipulates that service providers shall process training data in accordance with the law and improve data quality to enhance its authenticity, accuracy, objectivity, and diversity.

Data Governance

Focusing on AI data risk management and control, the core is to ensure the legality of training data sources and qualified data quality, and to prevent risks of non-compliant data usage and result bias.

System Accuracy, Reliability and Cybersecurity

The entire lifecycle of AI systems must ensure technical security, guarantee accuracy, reliability and stable operation, and guard against cybersecurity risks through technical means.

Transparency and Information Disclosure Requirements

Alleviate information asymmetry through transparency obligations, and fulfill duties including notification, disclosure and filing for relevant parties.

Organizational Governance and Risk Management

Establish an internal control and risk management system covering the full AI lifecycle, and achieve system controllability through key measures including internal control framework, risk assessment and personnel management.

User Rights

Clearly define that users of AI systems enjoy the rights to file appeals against adverse decisions, request manual review, and be free from algorithmic discrimination.

Prohibitions

Define the boundaries of unacceptable AI risks, and strictly prohibit the development and use of AI systems that endanger public interests and infringe upon legitimate rights and interests.

The Global AI Regulatory Landscape

2. System Accuracy, Reliability and Cybersecurity

AI systems are required to maintain an appropriate level of accuracy throughout their lifecycle and to guard against biases arising from operational environments as well as external attacks.

- Accuracy and Reliability: The system must achieve an appropriate level of accuracy for its intended purpose and be capable of effectively handling errors, disturbances, or anomalies that may occur in its operating environment. Technical and organizational measures must be implemented to ensure stable and reliable performance.

EXAMPLE: Article 15 of the EU Artificial Intelligence Act requires high-risk AI systems to maintain appropriate levels of accuracy, robustness, and cybersecurity throughout their lifecycle.

- Cybersecurity: Requires technical measures to resist malicious acts that exploit system vulnerabilities, such as adversarial attacks and data poisoning.

EXAMPLE: Section 5.4 of the Guidance for AI Adoption: Implementation practices(Australia) stipulates that AI systems need to implement robust data and cybersecurity measures to address AI-specific risks.

3. Transparency and Information Disclosure Requirements

Transparency obligations are designed to mitigate information asymmetry between AI providers and users. Currently, regulations focus on the following dimensions:

Transparency Toward Users:

- Prior Notification: When directly interacting with an AI system, users should be informed in an appropriate manner that the counterparty they are interacting with is an AI.

EXAMPLE: Article 31 of South Korea's Basic Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness stipulates that when providing generative AI products and services, AI business operators shall notify users in advance that such products and services are AI-generated.

- Explanation of Decisions: For decisions that are high-risk or affect users' rights and interests, explanations and descriptions of AI contribution should be provided.

EXAMPLE: Article 86 of the EU Artificial Intelligence Act provides that natural persons affected by a decision of a high-risk AI system have the right to request a clear and meaningful explanation from the deployer.

The Global AI Regulatory Landscape

- **Content Labeling:** Adding explicit or implicit identifiers to AI-generated content.

EXAMPLE: Section 22757.3 of the California AI Transparency Act stipulates that generative AI providers should embed implicit identifiers in generated content and provide users with the option to add explicit identifiers.

- **Public Disclosure:** Disclosing information via official channels regarding technical principles, training data, algorithmic discriminations, or registration and filing numbers.

EXAMPLE: Articles 7, 16, and 26 of China's Provisions for the Administration of Algorithmic for Internet Information Services stipulate that algorithm recommendation service providers shall disclose rules, basic principles, purposes and intentions, primary operating mechanisms, and filing numbers of algorithm recommendation services.

Transparency Toward Deployers:

- **Downstream Information Provision:** AI system developers should provide downstream deployers with key information such as the system's intended use, performance limitations, and human oversight conditions.

EXAMPLE: Singapore's Model AI Governance Framework for Generative AI requires AI model developers to disclose key information concerning training data, infrastructure, and evaluation results to downstream deployers.

Transparency Toward Regulators:

- **Regulatory Filing:** Requiring certain AI systems or services—such as high-risk AI systems or generative AI services with public opinion influence—to fulfill regulatory filing, registration, or submission of key materials such as assessment reports.

EXAMPLE: China's Provisions for the Administration of Algorithmic, Provisions on the Administration of Deep Synthesis of Internet-based Information Services and Interim Measures for the Administration of Generative Artificial Intelligence Services stipulate that algorithm recommendation, deep synthesis, and generative AI services with "public opinion properties or social mobilization capabilities" shall fulfill corresponding filing obligations. Laws in jurisdictions such as the EU and Vietnam clarify that high-risk AI systems must fulfill database registration and information update obligations.

- **Incident Reporting:** Reporting accidents (such as security incidents or algorithmic discrimination) to regulatory authorities after occurrence.

EXAMPLE: Section 1422 of New York's Responsible AI Safety and Education Act requires large-scale AI developers to fulfill reporting obligations within 72 hours of becoming aware of a safety incident.

The Global AI Regulatory Landscape

4. Organizational Governance and Risk Management

Companies are required to build internal controls to ensure that AI systems are effectively governed and controlled throughout their entire lifecycle.

- **Governance Framework:** An internal governance plan (e.g., quality management framework, risk management framework) should be developed for AI systems.

EXAMPLE: Article 7 of China's Provisions on the Administration of Deep Synthesis of Internet-based Information Services requires deep synthesis service providers to establish comprehensive information security management systems covering various aspects such as technological ethics, data security, and personal information. Article 17 of the EU Artificial Intelligence Act requires providers of high-risk AI systems to establish a quality management system covering stages such as design and verification, development and quality assurance, data management, and risk management.

- **Conducting Assessments:** Risk assessments, impact assessments, or security assessments should be conducted for AI systems.

EXAMPLE: Articles 32 and 35 of the South Korea's Basic Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness provide that AI providers shall conduct entire-lifecycle safety risk assessments for AI systems meeting the relevant thresholds, and that high-impact AI products or services shall conduct a basic human rights impact assessment in advance.

- **Human Oversight:** Human oversight mechanisms should be established to enable deployers to understand system operations and, when necessary, intervene or take over.

EXAMPLE: Article 20 of Brazil's Bill on the use of Artificial Intelligence stipulates that it should be ensured that human overseers are able to effectively understand, intervene in, and control high-risk AI systems.

- **Traceability:** Systems are required to include logging functions, and organizations should retain key evidence such as event records and technical documentation.

EXAMPLE: Articles 11 and 12 of the EU Artificial Intelligence Act impose strict technical documentation retention and logging obligations on entities ranging from providers and importers to deployers of high-risk AI systems.

- **AI Literacy:** Staff education is required to enhance their level of AI knowledge.

EXAMPLE: Article 4 of the EU Artificial Intelligence Act requires the providers and deployers of AI systems to ensure that their staff possess AI literacy aligned with their responsibilities.

The Global AI Regulatory Landscape

5. User Rights

Clear rights for AI system users are established, including the right to appeal against AI decisions, to request human review, to the right to non-discrimination, and so on.

- Right to Appeal: Users have the right to raise objections to adverse decisions and request human review. A small number of jurisdictions also allow users to opt out of AI decision-making.

EXAMPLE: Section 2.2 of the Guidance for AI Adoption: Implementation practices(Australia) stipulates that individuals or relevant parties affected by AI systems have the right to question AI decisions and usage behaviors, file appeals, and obtain human review and remediation. The relevant processes should be accessible, clear, and easy to understand.

- Right to Non-discrimination: Measures shall be taken to mitigate algorithmic discrimination based on protected characteristics such as race and gender.

EXAMPLE: Article 5 of the EU Artificial Intelligence Act provides that AI systems shall not implement algorithmic discrimination against protected characteristics such as race, religious belief, and sexual orientation, thereby safeguarding users' right to non-discrimination.

6. Prohibitions

Unacceptable risk boundaries are defined through prohibitive clauses, such as banning AI systems that employ subliminal manipulation, infer emotions in educational or workplace settings, exploit the vulnerabilities of vulnerable groups, or exhibit characteristics that pose clear societal harm.

EXAMPLE: Article 6 of China's Provisions on the Administration of Deep Synthesis of Internet-based Information Services explicitly prohibits deep synthesis services that endanger national security, the public interest, or the legitimate rights and interests of individuals.

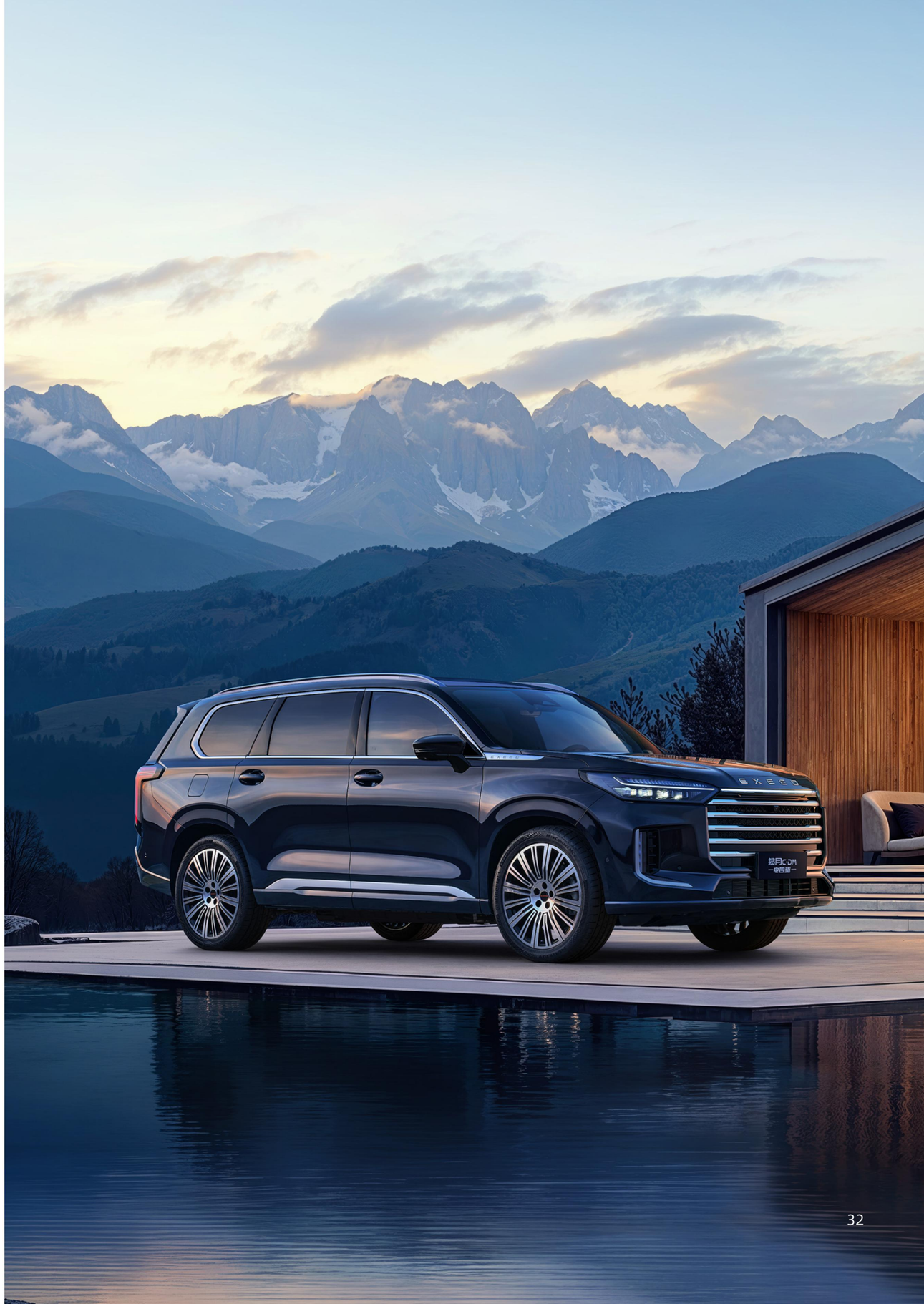
In addition to the aforementioned applicable requirements, major jurisdictions have also issued sector-specific regulations for enterprises in key industries such as automated vehicles, finance, and healthcare.

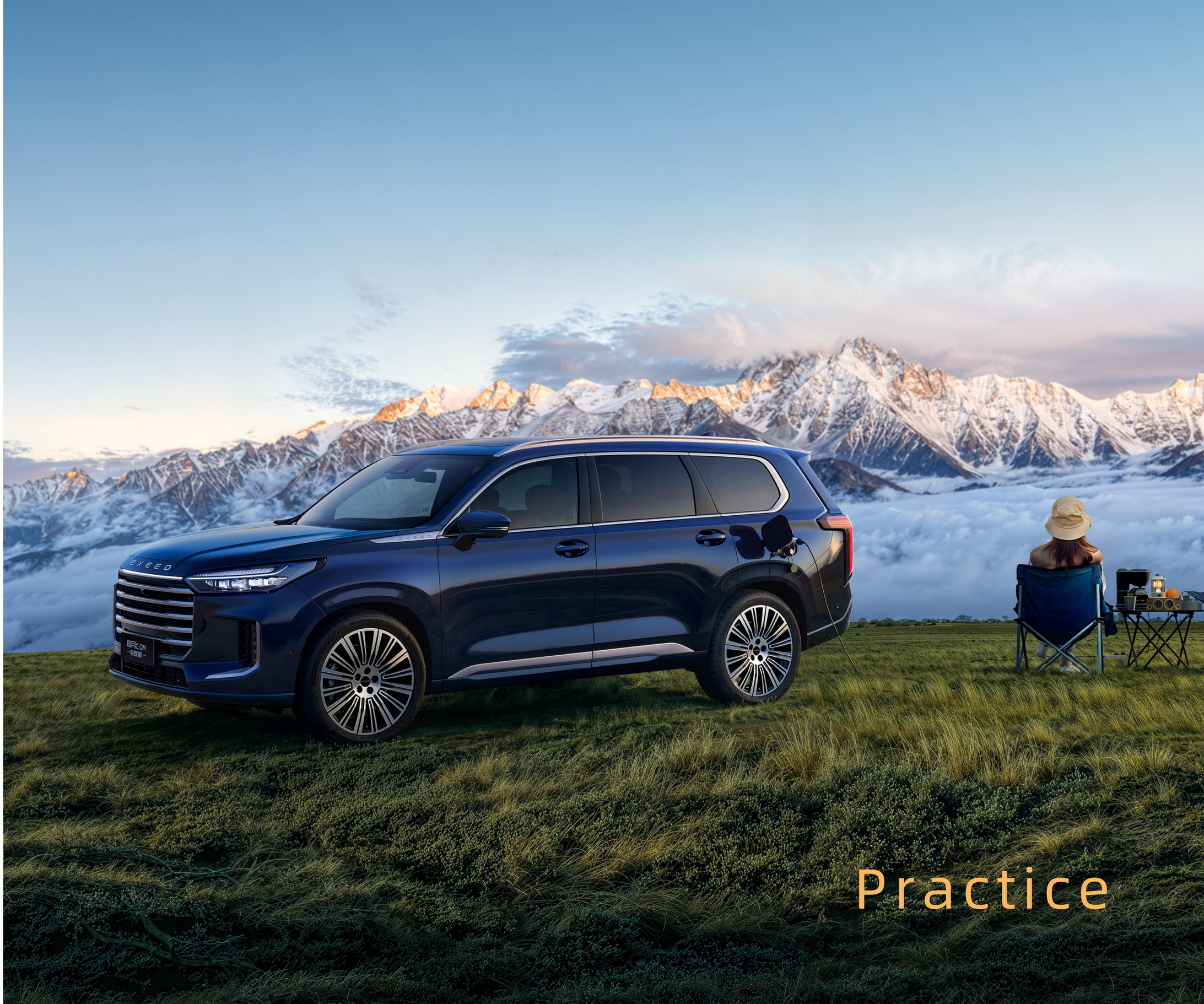
The Global AI Regulatory Landscape

III. Consequences of Non-Compliance

To ensure the implementation of regulatory requirements, legally binding "Hard Law" typically establishes explicit penalties. For example, the EU Artificial Intelligence Act provides that organizations failing to comply with the prohibition of the AI practices may be subject to fines of up to €35 million or 7% of annual global turnover, whichever is higher. For violations of requirements applicable to high-risk AI systems and most other non-compliance matters, fines may reach up to €15 million or 3% of annual global turnover, whichever is higher. China's Interim Measures for the Management of Generative Artificial Intelligence Services similarly specify that generative AI service providers in violation of the measures shall be subject to penalties in accordance with provisions in laws and administrative regulations on cybersecurity, data security, and the like. Where laws and administrative regulations do not provide for penalties, relevant authorities may issue warnings, public criticism, or orders for corrective action within a specified period; those who refuse to correct violations or whose violations are serious may be ordered to suspend the provision of relevant services. In contrast, violations of "Soft Law" generally do not directly trigger administrative penalties, but may be regarded as deviations from industry standards and best practices.

For enterprises, these regulatory requirements and the multifaceted consequences of non-compliance have created explicit compliance pressure. Accordingly, establishing a comprehensive AI governance and compliance framework has become an essential choice for enterprises.





Practice

CHERY 2026
DATA COMPLIANCE

AI Compliance Practices for Enterprises

I. Key Focus Areas for AI Compliance Practice

While AI compliance represents a new compliance domain, enterprises can build upon and integrate existing functions such as product development, information security and compliance, and operations and maintenance. In particular, the assessment mechanisms, transparency designs, internal control processes, and user rights response protocols developed through prior data compliance initiatives provide a solid foundation for advancing AI compliance in a coordinated manner.

We outline below seven key focus areas that enable enterprises to efficiently conduct AI compliance work and effectively fulfill AI regulatory requirements:

1. Data Governance: Establish an admission assessment regime for training, validation, and testing data. Review the lawfulness of data sources and personal data processing; also evaluate data relevance, representativeness, completeness, and accuracy to identify and correct biases and ensure that data quality standards are met.

2. System Reliability and Security Safeguards: Formulate and verify standards for model accuracy and reliability. Conduct targeted security testing for AI systems (such as red-teaming and penetration tests), implement targeted protections, and continuously monitor operational security.

3. Transparency and Information Disclosure: Meet information disclosure obligations for users, deployers, and regulatory authorities; implement user notification and content labeling; provide necessary technical and compliance documentation to deployers; and fulfill relevant regulatory reporting obligations.

4. Establishment of Internal Governance: Set AI governance frameworks and internal control processes, and implement risk assessment, human oversight, and traceability mechanisms, and enhance employees' AI literacy.

5. Protection and Redress of User Rights: Improve channels for responding to user rights requests and providing remedies, and prevent AI system decisions from discriminating against users through product design.

6. Review of System Use Cases: Make internal rules for restricted and prohibited AI use cases. New AI systems shall undergo use-case review before launch, and for existing systems on a regular basis. For any system found to involve prohibited use cases, implement remediation measures or terminate operation as appropriate.

7. Monitoring Regulatory Dynamics: Track global legislation and enforcement developments, analyze regulatory trends, and adjust product design and compliance strategies accordingly.

AI Compliance Practices for Enterprises

II. AI Compliance Practices of Leading Enterprises

1. The Evolution of AI Governance in Leading Enterprises

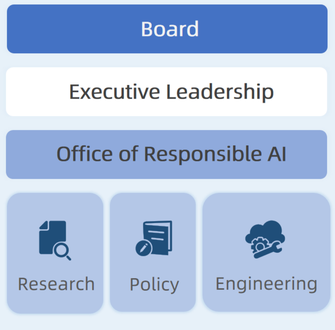
To date, leading enterprises have established relatively comprehensive AI governance frameworks. Taking a large U.S. technology company as an example, it began its "Responsible AI" framework-building journey in 2018 and is now widely regarded by the industry as a benchmark for AI compliance.

Leading Practice: The Path of Building a "Responsible AI" System at a Large Technology Company

Since 2018, the company has systematically advanced its "Responsible AI" program in three stages:

Stage I: Establishment of Principles (2018)

Published six AI principles, including fairness, reliability, privacy, and inclusiveness, among others, laying the value foundation for all subsequent work.



Stage II: Governance System Construction (2018–Present)

Centered on these principles, the company constructed a multi-layered governance system integrating organization, processes, and tools:

- **Policies and Frameworks:** Issued the corporate-level Responsible AI Standard to clarify requirements across the entire lifecycle. Its risk management framework is aligned with the NIST AI Risk Management Framework (AI RMF) to manage generative AI risks.
- **Governance Architecture:** Formed a governance architecture overseen by the Board of Directors, coordinated by cross-functional committees, with the Office of Responsible AI serving as the core executive body.
- **Tool Construction:** Disclosed service information through Transparency Notes and provided customers with compliance tools.
- **Talent and Community:** Established an internal Responsible AI community of hundreds of people, with a 99% completion rate for mandatory AI literacy courses.
- **Social Impact:** Continuously funded frontier research, actively participated in global multi-stakeholder governance dialogues, and promoted AI governance practices in the industrial ecosystem.

Stage III: Launch of Compliance Work (2024–Present)

In response to the latest regulations such as the EU Artificial Intelligence Act, its governance system demonstrates agile adaptability:

- **Addressing Prohibited Practices:** Conducted screening of existing systems, while updating internal policies, marketing guidelines and contractual terms to ensure business-wide compliance.
- **Enhancing AI Literacy:** Systematically constructed an AI knowledge center, customized courses for employees, and made training resources available to the public.
- **Compliance Preparation for General-Purpose AI (GPAI) Models:** Added model-level policies to the development process, established automated documentation processes, and communicated with EU regulators to prepare for GPAI rules to take effect.

* The information in this case is compiled from the company's publicly disclosed 2024 Responsible AI Transparency Report and 2025 Responsible AI Transparency Report.

AI Compliance Practices for Enterprises

2. Practical Experience in AI Compliance from Leading Enterprises

The leading AI governance and compliance practices provide valuable insights for enterprises still in the exploratory stage, including:

First: Anchoring full-lifecycle risk management in governance principles.

Embed risk management throughout the full lifecycle of AI system design, development, deployment, and operation, thereby building a stable compliance foundation. This approach closely aligns with the regulatory consensus across jurisdictions regarding full-lifecycle AI risk management, enabling enterprises to leverage this common mechanism as a foundation to meet the core regulatory requirements of different jurisdictions.

Second: Ensuring implementation through an institutionalized governance architecture.

Through a governance architecture comprising Board oversight, cross-functional committee coordination, and execution by the Office of Responsible AI, enterprises establish clear and institutionalized chains of responsibility and key decision-making checkpoints to achieve comprehensive risk management across the entire lifecycle of AI system development and operation. This institutionalized and organizational approach ensures that governance principles are effectively implemented and embedded throughout the organization.

Third: Supporting continuous operation through engineering tools and organizational evolution.

By developing automated tools and standardized documentations, leading enterprises operationalize AI compliance requirements and improve efficiency and traceability. Beyond tools, organizational evolution is equally important: the continuous operation of internal AI communities, the development of employee literacy, and effective communication with the authorities equip the governance system with the adaptability required for continuous operation.

Leading enterprises' AI governance systems were not achieved in one stroke according to a pre-drawn blueprint; rather, they "grew" gradually through the ongoing process of addressing practical challenges. From issuing governance principles and constructing governance frameworks, to launching compliance responses, leading enterprises have undergone years of iteration and accumulation, progressively achieving three critical transformations: embedding governance requirements into development processes, integrating governance responsibilities into the organizational structure, and internalizing a sense of responsibility into employee competencies. Through this evolution, "Responsible AI" has transitioned from a time-bound initiative into an organizational operating capability. This process offers no shortcuts; it demands sustained investment and continuous experimentation to develop a governance system that genuinely aligns with the enterprise's unique logic and context.

AI Compliance Practices for Enterprises

III. Chery's AI Compliance Practices

Established in June 2024, NEXTAI is Chery's core institution for intelligent technologies. With a vision of "AI Reshaping an Efficient Future," NEXTAI is designed to be the pioneer driving the group's comprehensive digital transformation driven by innovation and global credibility. NEXTAI focuses on frontier exploration in AI, innovative technologies, and scenario-based digital applications, and remains committed to embedding AI compliance concepts into the entire AI lifecycle, achieving a series of phased practical outcomes.

Case 1 **NEXTAI-Coder: Intelligent Programming Assistant:** By using high-quality open-source datasets for model training and taking stringent measures to avoid intellectual property infringement, NEXTAI ensures the quality and compliance of training data at the source.

Case 2 **Intelligent BOM Review Platform for Parts:** Leveraging Chery's proprietary 3D digital models and BOM lists as training data to fully ensure the sovereignty and legal compliance of underlying data sources.

Case 3 **NEXT-Ada Deep AI Agent Platform for High-Frequency Tasks:** Enforcing strict access controls and data isolation to secure internal data when deploying AI agents for high-frequency tasks like meeting management, document processing and coding, preventing unauthorized access or leakage.

Case 4 **Component Cost Deep Mining AI Platform:** Leverage large models and encrypted databases to safely disassemble the costs of black-box and gray-box components. Core data and procurement pricing logic are isolated and computed only on the internal network to strictly prevent confidential data leakage.

Case 5 **Intelligent Talent Discovery Assistant:** By prioritizing competency profiles, project experience, and performance data as core evaluation dimensions, while strictly excluding non-professional factors such as age, gender, or marital status—the system ensures fair recruitment.

Case 6 **AI for CAE Physics Simulation Platform:** Establishes a version traceability mechanism for simulation AI models, ensuring that modifications of physical prediction data (such as Body in White stiffness and wind noise) are tracked in a tamper-proof manner, achieving full-process traceability.

Case 7 **DevOps Intelligent Monitoring Platform:** Provides full-process intelligent monitoring of the production line; sets up manual review checkpoints for high-risk actions such as fault self-healing and configuration changes, thereby enabling effective supervision of AI operations activities.

Case 8 **AI Empowerment Training:** Conducted over 40 AI empowerment training sessions, covering all core business units and functional departments, with participation exceeding ten thousand person-times; jointly launched the AI Evangelist Development Program with Chery University to enhance AI literacy across the entire workforce.

Case 9 **AI Compliance Admission Evaluation Process:** Established an AI model and application compliance admission mechanism, conducting assessments of the legality of training data sources, model ethical risks, and algorithm filing obligations, thereby ensuring the compliant launch of AI models and applications.

NEXT AI

AI Compliance Practices for Enterprises

IV. Future Challenges of AI Compliance Practice

We anticipate that AI compliance work will face the following core challenges in the future.

1. Complexity of the Regulatory Environment

Global enterprises are confronted with a multidimensional regulatory matrix shaped by horizontally unified legislation, vertically segmented regulation, and territorial jurisdiction. Rules across jurisdictions may differ significantly. For example, the training data used for the same model may fall within a copyright exception in jurisdiction A, but may constitute infringement in jurisdiction B. In addition, global regulatory rules remain in a period of frequent evolution, with enforcement approaches continuing to adjust dynamically, further increasing the difficulty of AI compliance.

2. Regulatory Uncertainty for New Technological Paradigms

The pace of iteration in AI technological paradigms outstrips the pace of regulatory updates, leaving many new applications of AI in a state of regulatory ambiguity. This requires enterprises to independently assess compliance risks when applying innovative AI technologies and to establish internal control mechanisms capable of adapting dynamically to technological change.

3. Difficulty of Full-Lifecycle Risk Management

Embedding risk management throughout the full product lifecycle necessitates the transformation and restructuring of existing research, development, and operations systems, the deployment of corresponding tools, and the integration of compliance checkpoints into each stage of data collection, model training, deployment, and continuous monitoring. The core challenge lies in ensuring that risks remain manageable and controllable while preventing compliance processes from impeding agile business iteration.

4. Shortage of Professional Resources

Addressing all of the foregoing challenges depends on interdisciplinary talent with both regulatory and technical expertise, as well as mature solutions. However, expert-level talent remains scarce in the current market, solutions tailored to complex business scenarios are insufficient, and enhancing internal AI literacy within enterprises requires sustained investment of time and resources. These factors have become key constraints on the effective implementation of enterprise AI compliance strategies.

Envision

CHERY 2026
DATA COMPLIANCE

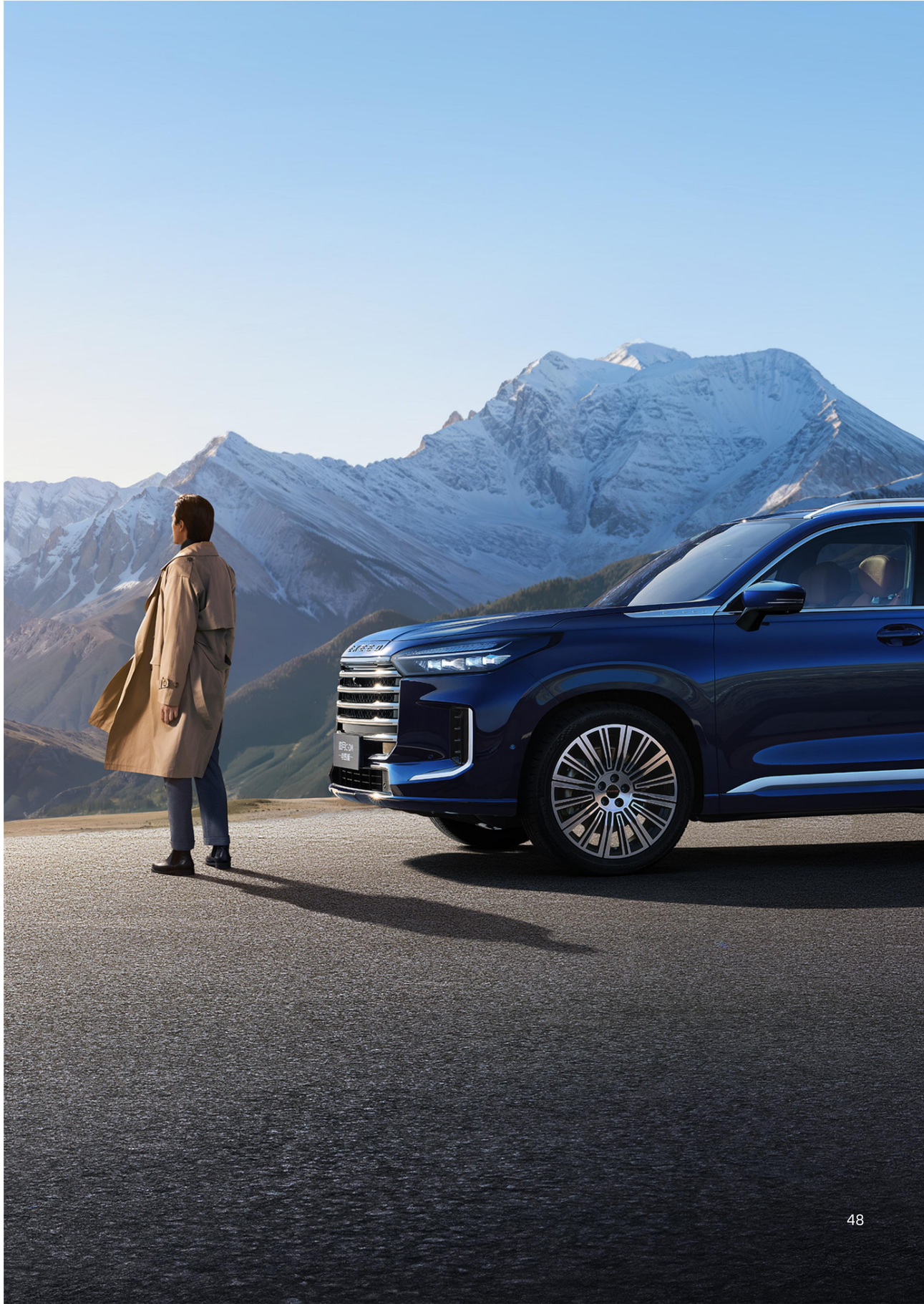
Envisioning AI Compliance at Chery

AI has entered an era of institutionalized regulation. Facing the complex risks and far-reaching implications brought by rapid technological evolution, major jurisdictions are accelerating the construction of regulatory policy frameworks.

Against this backdrop, enterprises urgently need to build systematic AI governance and compliance capabilities, embed risk management throughout the entire lifecycle of AI systems, and substantively address regulatory requirements across major jurisdictions in areas including data governance, system accuracy and reliability, cybersecurity, transparency, organizational governance and risk management, user rights protection, and prohibitive requirements.

Since Chery launched various AI projects, our objective extends beyond merely satisfying current regulatory compliance requirements. More importantly, through systematic construction, we aim to progressively transform AI governance into an organizational core function, ensuring that the compliance of new technologies such as AI ultimately becomes ingrained in the enterprise's DNA and translates into user trust and brand reputation.

AI compliance governance is a process that requires sustained investment, continuous iteration, and long-term accumulation. As an industry participant, we are committed to exploring alongside the broader industry, sharing experiences and insights, advancing the maturation of AI governance practices, and becoming a steadfast force driving the industry toward the greater good.



CHERY 2026
DATA COMPLIANCE

Appendix

Appendix: AI Regulatory Instruments in Major Global Jurisdictions

China

Provisions for the Administration of Algorithmic

Provisions on the Administration of Deep Synthesis of Internet-based Information Services

Interim Measures for the Administration of Generative Artificial Intelligence Services

Measures for the Labelling of Artificial Intelligence-Generated and Synthetic Content

Cybersecurity Technology-Labeling Method for Content Generated by Artificial Intelligence

Cybersecurity Technology—Basic Security Requirements for Generative Artificial Intelligence Service

Hong Kong, China

Generative Artificial Intelligence Technical and Application Guideline

Taiwan, China

Artificial Intelligence Fundamental Act

United States of America

California

AI Transparency Act

Transparency in Frontier Artificial Intelligence Act

Generative Artificial Intelligence: Training Data Transparency

Companion Chatbot Law

New York

Responsible AI Safety and Education Act

Colorado

Consumer Protections for Artificial Intelligence

Texas

Responsible Artificial Intelligence Governance Act

European Union

Artificial Intelligence Act

Guidelines on the definition of an Artificial Intelligence system

Guidelines on prohibited Artificial Intelligence (AI) practices

Guidelines for providers of general-purpose AI models

The General-Purpose AI Code of Practice

United Kingdom

A pro-innovation approach to AI regulation

Appendix: AI Regulatory Instruments in Major Global Jurisdictions

Other Region

Japan

Act on Promotion of Research and Development, and Utilization of Artificial Intelligence-related Technology

Guideline for Ensuring the Appropriateness of Research & Development and Utilization of Artificial Intelligence-Related Technology

South Korea

Basic Act on the Development of Artificial Intelligence and the Establishment of Foundation for Trustworthiness

Guideline on Processing of Personal Information in Developing and Using Generative AI

Singapore

Model AI Governance Framework for Generative AI

Vietnam

Law on Artificial Intelligence

India

AI Governance Guidelines

Kazakhstan

On Artificial Intelligence

Saudi Arabia

Generative AI Guidelines for the Public

United Arab Emirates

AI Ethics Principles and Guidelines

Qatar

Principles and Guidelines for Ethical Use of Artificial Intelligence

Turkey

Artificial Intelligence Law Bill

Australia

Guidance for AI Adoption: Implementation practices

New Zealand

Responsible Artificial Intelligence Guidance for Businesses

Canada

Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems

Brazil

Bill on the use of Artificial Intelligence

Argentina

Legal regime for the responsible use of AI

El Salvador

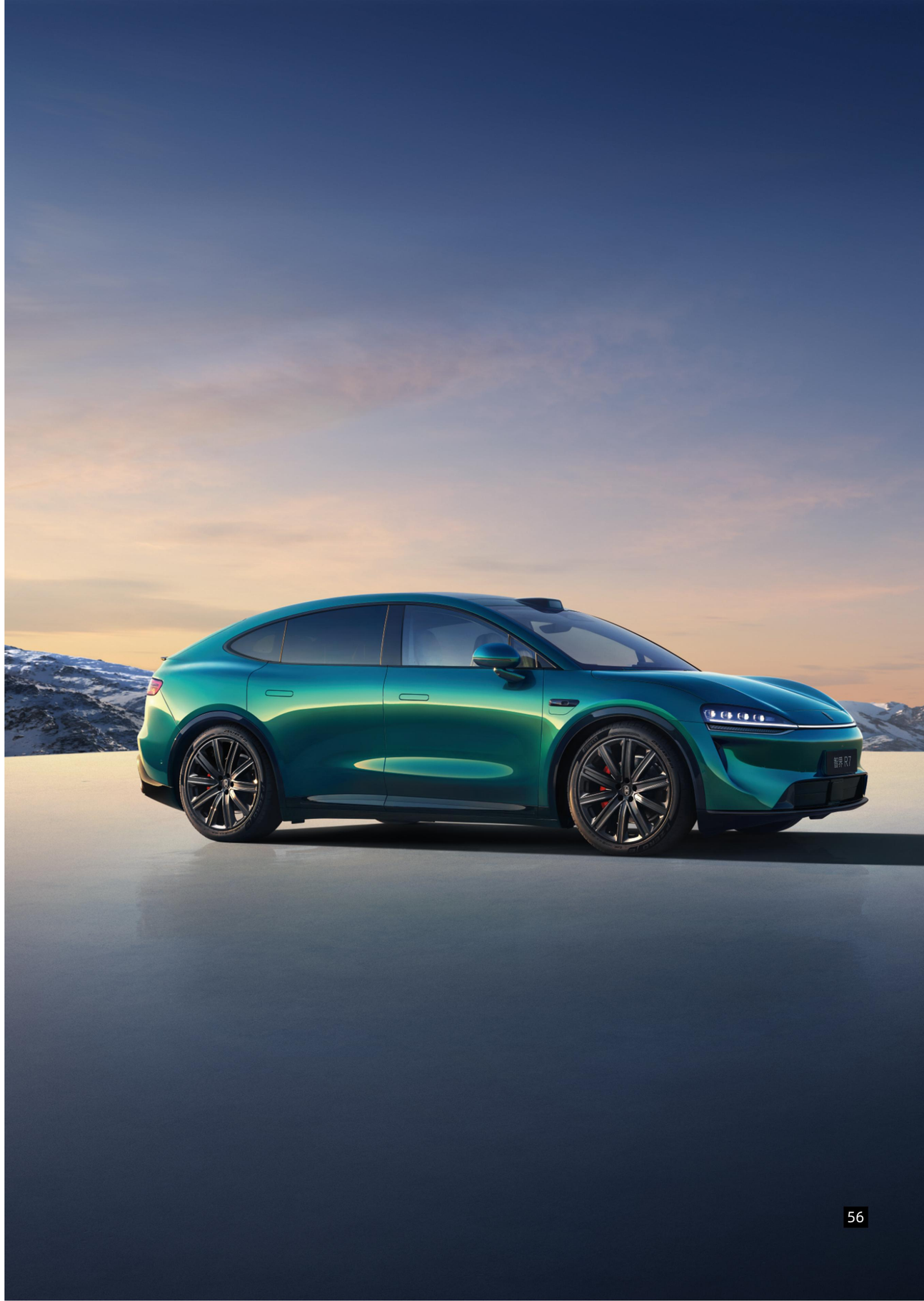
Law For The Promotion Of Artificial Intelligence And Technologies

Disclaimer

This white paper is authored by Chery Automobile Co., Ltd. ("Chery"). Chery independently holds the intellectual property rights to the content it has contributed. All text, data, images, and tables contained within this document are protected under the Copyright Law of the People's Republic of China and other relevant laws and regulations. Without the written permission of Chery, no organization or individual is permitted to use the information in this report (including the entirety or any part thereof) for any commercial purpose, nor to excerpt, copy, store in retrieval systems or disseminate it in any form or by any means (including electronic, mechanical, photocopying, recording, or scanning).

The information in this document is sourced from data collected during this survey and publicly available materials. We make no guarantees or warranties regarding the completeness, accuracy, or timeliness of the information, nor do we offer any express or implied warranties, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose. Opinions may vary from those presented in this report at different times.

This document is for general reference only and does not constitute specific matters or consulting opinions. It does not provide any form of legal advice, accounting services, investment recommendations, or professional consultations. The information provided in this document cannot replace professional tax, accounting, legal advice, or other related professional consulting suggestions. Chery does not assume any fiduciary responsibility for the content of this report. Chery does not assume any responsibility or obligation to any person for the content of this report, nor does it assume any responsibility or obligation arising from or related to this report. Readers should not rely on the content of this document to make investment or other business decisions. For specific opinions, please consult professional advisors.



DIT | NEXTAI

Editors-in-Chief

Dai Chuang, Mo Dalin, Li Yi, Zou Jiaqi, Ding Yanzhong

https://m.weibo.cn/u/2005342162

https://www.facebook.com/cheryinternational

https://www.youtube.com/@cheryinternational_official