

WHITEPAPER

AI Agents from China

© Copyright 2025 CHINABRAND IP CONSULTING GMBH



AI agents represent one of the most exciting developments in artificial intelligence in China. An AI agent is a software system capable of perceiving its environment, processing information, and independently performing actions to achieve specific goals. It acts as an intelligent assistant, operating autonomously and undertaking tasks without human supervision. AI agents can learn, adapt, and seamlessly interact with other technologies, fundamentally transforming how we work, live, and communicate with our environment.

Types of AI Agents

There are two types of AI agents: rule-based and learning-based. Rule-based agents follow fixed rules and are ideal for simple, repetitive tasks. Classic examples include chatbots in customer support that use predefined scripts to answer frequently asked questions. While reliable for routine queries, their functionality is limited to programmed scripts. In contrast, learning-based AI agents utilize machine learning to continuously improve. They analyze past interaction data, identify patterns, and generate personalized, context-specific responses. Examples include recommendation algorithms used by platforms like Netflix and Spotify.

Modern AI agents merge the strengths of both approaches. The rule-based component ensures predictability and clear, repeatable processes, while the learning-based component enables the agent to respond flexibly to new information. This combination significantly enhances their capabilities, contributing to their increasing adoption. By 2025, AI agents have reached new levels of performance, thanks to advancements in machine learning and increased computing power, notably via cloud computing. They can manage complex, data-driven tasks continuously, significantly boosting productivity and reducing human error. Improved algorithms and extensive data also allow for comprehensive personalization, customizing user experiences through tailored product recommendations, optimized business processes, or superior customer support, revolutionizing business operations.

A traditional rule-based AI agent follows a fixed procedure. It is triggered by a specific action, such as a customer opening a chat window on a website. The agent then processes input by scanning for keywords indicating a particular issue. Based on these keywords, it selects a response from predefined options, providing standardized answers. This method functions well as long as the customer adheres to the anticipated conversation pattern; deviations require human intervention.

Conversely, modern AI agents employ more dynamic approaches. They leverage advanced natural language processing (NLP) to understand context, sentiment, and intent, enabling more flexible interactions. For example, an AI agent might analyze

previous customer interactions to predict potential issues, then formulate personalized responses beyond standard replies. Continuous learning from feedback and external databases or CRM systems further enhances responsiveness. UDESK, a Chinese online customer service platform, exemplifies this approach, integrating AI-powered chatbots, multi-channel communication, and customer service management.



Significant advancements differentiate modern AI agents from earlier systems. While traditional agents were static and rule-based, modern agents combine fixed rules with machine learning and NLP, allowing contextual responsiveness and continuous evolution. Another significant improvement lies in personalization, with modern AI agents designed to offer customized experiences by storing user histories and learning from past interactions.

Developing AI Agents

The development of AI agents begins with defining their objectives—whether answering customer inquiries, recommending products, or assisting in programming tasks. Python remains widely used in China due to its extensive libraries for AI development, including the powerful Hugging Face Transformers for NLP.

Alternatively, no-code platforms such as Google Dialogflow or IBM Watson facilitate AI agent creation without programming expertise. In China, platforms like Baidu Miaoda (百度)

度秒哒), Relevance AI, and Lecca are prominent, along with cloud providers Alibaba Cloud, Tencent Cloud, and Baidu AI Cloud, offering robust AI services for businesses.

When designing AI systems, key considerations include:

- How does the agent collect information?
- How does it process the information?
- What criteria does it use for decision-making?
- How does it provide appropriate responses?

Data quality is essential for effective AI agent performance. International platforms like Kaggle and Chinese platforms like Whale Intelligence Community (鲸智社区), Baidu AI Studio (飞桨 AI Studio), DataCastle (数据城堡), and Alibaba Cloud Tianchi (阿里云天池) offer extensive datasets crucial for training and optimization.

Deployment of Chinese AI Agents

Western companies operating in China will adopt Chinese AI agents to maintain competitiveness in the local market. However, China will also export autonomous AI agents globally. The deployment of Chinese AI agents offers significant efficiency gains but presents substantial challenges:

- **Sensitive Data:** AI agents often access sensitive data such as customer information.
- **Data and Cybersecurity Regulations:** Laws restrict AI usage, especially concerning cross-border data transfer.
- **Algorithm Transparency Requirements:** Chinese regulations frequently mandate algorithm disclosures, potentially risking trade secrets.
- **Competition Law:** AI algorithms must not facilitate implicit price agreements or abuse market dominance.
- **Liability Issues:** Accountability for erroneous AI decisions remains unclear, particularly regarding autonomous systems.

A critical aspect involves sensitive data handling. Given China's extensive data control regulations, European companies face challenges ensuring data security and confidentiality. Cross-border data transfer is especially sensitive due to stringent European data protection regulations (GDPR), potentially conflicting with Chinese laws.

Chinese data security laws, notably the Data Security Law and Cybersecurity Law, have created a highly regulated environment, causing uncertainties for companies outside

China, particularly regarding cross-border data flows. Concerns also persist over potential hidden vulnerabilities in Chinese AI agents.

Transparency of AI algorithms remains another critical concern. Mandatory algorithm disclosures under Chinese law pose significant risks to European businesses and investors due to potential exposure of proprietary technologies.

Competition law issues also pose challenges. Chinese regulators have intensified efforts against monopolistic practices, yet concerns persist about AI-driven market manipulation by leading tech firms like Alibaba, Tencent, and ByteDance. European regulatory authorities may scrutinize imported Chinese AI agents rigorously to prevent market distortion.

Lastly, liability remains unresolved. Clarifying responsibility for faulty decisions made by autonomous AI agents—whether manufacturer, operator, or end-user—is crucial, especially in sensitive sectors like healthcare, finance, or autonomous driving.

Overall, deploying Chinese AI agents presents substantial opportunities alongside complex challenges. European companies must thoroughly assess risks, considering regulatory, ethical, and security challenges, and develop a profound understanding of China's political and economic context to maintain competitiveness and compliance.

For Further Informations

For more Informations about our services, please visit:

www.chinabrand.de

Contact und Feedback

info@chinabrand.de

Blog | LinkedIn

© Copyright 2025 CHINABRAND IP CONSULTING GMBH. All rights reserved.

Grashofstraße 3, 80995 München - +49 89 321212800 - www.chinabrand.de