China discusses restrictions on open-weight AI models

19:37

Yes, the Chinese government is currently considering far-reaching restrictions on access to its most advanced AI models, particularly with regard to their release as so-called 'open-weight' models to foreign countries. [1, 2]

This marks a potential U-turn in Beijing's AI strategy. Whilst
Chinese companies such as Alibaba (with the Qwen family) or start-ups such as *Z.ai* and *Moonshot AI have* recently been aggressively flooding the market with powerful open-weight
models, national security interests are now taking centre stage. [1, 2, 3, 4, 5, 6, 7]

An overview of the key details of the discussions:

The planned tiered system

Following reports of confidential talks between the Chinese Ministry of Commerce and tech giants such as ByteDance, Alibaba and Z.ai, a **tiered regulatory system** is under discussion: [1, 2, 3]

- **Simple models:** Basic open-source AI is to remain freely available following a simple registration or sign-up process.
- **Advanced models:** More powerful technologies must undergo strict security checks in advance.
- **Frontier models:** The most powerful, as yet unpublished AI systems are to be **completely blocked from public access and from overseas**, or restricted to purely domestic use. [1, 2, 3]

What does this mean for 'Open Weight'?

The essence of Open Weight models lies in the fact that users can download the trained parameters and run the AI locally on their own servers independently. [1]

- **No withdrawal of data already published:** Once downloaded, models (such as older versions of Qwen or Kimi) can no longer be technically retrieved by China retrieved. [1, 2]
- **Future as a closed API:** For future state-of-the-art models, Beijing is considering completely banning the download of model weights for foreign users
  . Instead, these models could only be offered abroad in a controlled manner as a cloud service (API) in order to halt uncontrolled
  technology transfer. [1]

The background: the tech war with the US

The discussions in China are a direct response to the US government's tightened export controls and sanctions plans by **the US government**. As the US is massively restricting the export of cutting-edge chips and access to top-of-the-range US models for China, Beijing wants to prevent Western companies and developers from benefiting free of charge from China's own rapid advances in AI. Furthermore, unauthorised leaks of protected AI technologies are to be severely punished in future under the National Security Law. [1, 2, 3, 4, 5, 6]