If your team is exploring China-native AI tools, the first question is usually: "Do we need a +86 number?"

The short answer is: **it depends on the platform and region policy**.

This guide is intentionally neutral and compliance-first. It is not a circumvention tutorial. Use it to decide whether your access path is operationally sustainable and policy-aligned before you commit engineering time.

> **Scope and date:** Access behavior can change quickly. All checks in this post are based on publicly visible flows observed on **February 20, 2026**.
>
> **Verification method (date + environment):** Login/access checks were run on **February 20, 2026 (UTC+8)** using live browser verification (Playwright + manual checks) against the public login pages for DeepSeek, Doubao, Kimi, and Z.ai.

60-second takeaway

- **Not all China AI products require +86.** Some flows support email or federated login.
- **Some platforms are region-gated** and default to +86 phone onboarding.
- A +86 virtual number can solve only one layer (OTP reception), not policy, billing, geolocation, or account risk.
- The highest-risk mistake is treating an account setup workaround as a durable production access strategy.

1 Access matrix (observed, February 20, 2026)

Platform	Publicly visible login signal	+86 required? (observed)	Confidence	Verification date
DeepSeek (chat.deepseek.com)	Sign-up page shows an email route in our region; sign-in field allows phone/email input	**No (email path observed)**	High	2026-02-20

Doubao (doubao.com)	Region-ban page + login modal with China-region phone code options (+86, +852, +853, +886)	**Yes for the observed phone-login flow**	High	2026-02-20
Kimi (kimi.com)	Public landing/chat accessible; login offers Google plus phone flow (default +86)	**No strict +86 requirement observed**	High	2026-02-20
Z.ai (chat.z.ai)	Auth page offers Google, Email, GitHub, and Skip for now; manual checks also observed phone login with non-China country codes	**No**	Medium	2026-02-20

Interpretation notes:

- "No" does not mean every feature, region, or enterprise path is available without additional verification.
- "Yes for the observed flow" does not mean all users will see the exact same gate. Device, locale, IP region, and A/B experiments can change UX.

2 Why "+86 access" is often misunderstood

Teams usually bundle four separate constraints into one problem:

1. **Identity/OTP constraint:** Can we receive verification codes?
2. **Policy constraint:** Do terms allow this access path from our region/use case?
3. **Operational constraint:** Can we keep the account active and recoverable?
4. **Data-governance constraint:** Are we comfortable with KYC and data-sharing terms?

A +86 number can help with #1 in some scenarios. It does not automatically solve #2 to #4.

3 Optional path: virtual +86 via eSender (what it does and does not do)

One documented option is a Mainland China virtual number via eSender in WeChat.

What this path is useful for:

- Receiving OTP/SMS in WeChat for supported services.
- Bootstrapping account setup where a phone number is mandatory.

What this path does not guarantee:

- Eligibility under a platform's terms of use.
- Access to all product features.
- Stable long-term account durability.
- Peer-to-peer SMS behavior equivalent to a physical SIM.

Important operational details from vendor documentation:

- eSender Mainland numbers are not physical SIMs and run via WeChat official account workflow.
- Receiving SMS depends on active service period/package state.
- Real-name verification and identity document submission are part of the flow.
- Vendor terms explicitly describe personal-data handling tied to registration with relevant authorities.

If you use this route, treat it as a controlled experiment and document all assumptions in your internal runbook.

4 Compliance and risk checklist (before your team scales usage)

A) Terms and policy check

- Confirm each target platform's current terms and regional restrictions.
- Ensure your intended use (personal vs commercial vs API automation) is allowed.
- Define a stop condition if policy interpretation is ambiguous.

B) Identity and privacy check

- Decide whether your team is comfortable with KYC requirements and data-sharing disclosures.
- Minimize who can access identity documents and account-recovery channels.
- Record where identity artifacts are stored and retention period.

C) Operational resilience check

- Test OTP receipt reliability across multiple days and times.
- Test recovery scenarios (lost device, expired service period, re-verification).
- Set renewal reminders for any paid validity plans tied to the number.

D) Security and ownership check

- Use role-based ownership for shared business accounts.
- Store credentials and recovery steps in your secure secrets workflow.
- Avoid single-person account ownership for production-critical workflows.

5 Recommended rollout sequence (pragmatic)

1. **Shortlist platforms by business value** (not by hype).
2. **Validate access policy first** on official docs/support pages.
3. **Run one bounded access pilot** with clear success/failure criteria.
4. **Document risks and controls** before expanding usage.
5. **Only then automate** workflows or connect downstream operations.

6 Publish-safe stance for teams

A strong operating principle is:

> **If your access method is hard to explain in one compliance memo, it is too fragile for production.**

For most teams, the right decision is to prioritize platforms where account provisioning, billing, and policy posture are all explicit and repeatable.

Sources

- DeepSeek sign-in page
- DeepSeek sign-up page
- Doubao region restriction page
- Kimi homepage
- Z.ai chat homepage
- Z.ai auth page
- eSender FAQ (Mainland/HK number behavior)
- eSender official site
- Multibyte real-name policy