

API 中转属于刑事犯罪?境外 AI 还能用吗

作者: 朱晓阳 | 邓梓珊

2026 年 5 月, 上海某 API 中转站的经营者发帖, 称自己被上海警方刑事拘留 37 日后转为取保候审。其在公开声明中承认, 通过非法技术手段获取境外大模型 API 接口并转售国内用户, 目前已退赔退赃, 后续将面临罚金, 且“肯定是要判刑的”。

该事件并非孤例。消息发布后, 行业内部出现普遍担忧, “听说有人被带走”的询问在开发者社群中频繁出现, 部分运营者紧急停止服务, 亦有从业者主动退群。当第一批以 API 中转为主要盈利模式的经营者开始面临刑事追诉, 一个核心问题摆在所有从业者与用户面前: API 中转站的商业行为, 触及了哪些法律红线?

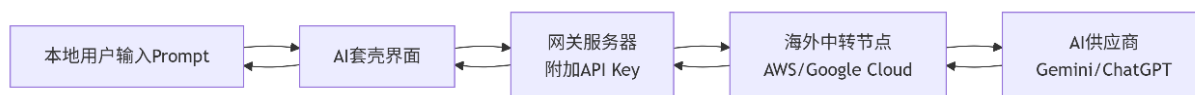
一. API 中转站的技术原理与盈利模式

API 中转站本质上是一个 **API 网关与聚合转发服务平台**, 核心功能是充当用户与第三方大语言模型 (LLM) 供应商 (如 **OpenAI、Google 或 Anthropic**) 之间的数据中转桥梁。在这个平台架构中, 面向用户的部分被称为“前端”或者“AI 套壳”, 通常是独立开发的应用、网站、或聊天界面。底层的技术结构被称为“后端”或者“API 网关”, 负责接收本地用户的输入并将其包装成标准化的请求, 然后通过 API (应用程序接口) 发给海外的官方 AI 服务器。

API 中转模式中, 数据流转主要分为四个阶段。首先, 处于服务器受限地区, 无法直接访问境外模型的本地用户在 AI 套壳界面上输入 **Prompt (提示词)**。然后, 网关服务器在接收到本地用户的请求后, 会附加合法的身份凭证 (API Key), 并通过在北美、欧洲等海外节点进行流量中转。随后, 境外的 AI 供应商收到请求, 并将其识别为来自合法云端开发者的使用。最后, 境外模型生成的原始文本将会返还给网关, 再经网关格式化处理后, 返还给本地用户。

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com



用户之所以选择该路径，原因在于在中国境内直接使用境外 AI 存在三重障碍：网络访问不稳定、需要境外信用卡支付、各模型接口格式不统一。API 中转站同时解决了上述问题——在境外部署服务器以规避网络限制，批量采购额度以支持支付宝/微信充值，利用 One API 等工具将不同模型统一为兼容格式。

从盈利模式看，API 中转站的利润来源可分为“合法优化”与“灰色操作”两类。

合法优化模式，运营者利用官方 API 的机制降低成本。例如，使用付费企业级 API Key，绑定企业级信用卡，严格按照实际花费的代币(Token)量进行付费；或通过 Prompt Caching(提示缓存)复用用户相同的系统提示词，享受官方提供的 50%至 90%折扣，但向前端用户按全价收费，赚取差价。

与之相对的则是“灰色操作”及非正规的运营模式，常见手段包括：

- **号池复用**：这种模式主要利用自动化脚本程序批量注册境外 AI 平台的免费账号，并利用网络爬虫技术抓取这些免费账户在浏览器中的对话。在该模式下，内部通常存在一个免费账户池，系统会轮流使用其中的账号直到免费额度耗尽。
- **非法方式获得 API Key**：通过黑色渠道购买官方 API Key，例如使用在暗网流通的盗刷信用卡或拒付卡，直到盗刷的信用卡被冻结或者发生银行拒付。另一种机制是通过网络爬虫程序抓取在互联网上开源项目意外暴露的 API Key 并使用。也有直接盗取订阅了 AI 服务企业账户从而获取 AI 供应商的算力或者通过“钓鱼”手段，比如使用虚假的 AI 开发项目来诱骗正规开发者的 API Key。
- **逆向中转**：将 ChatGPT Plus 或 Claude Pro 的网页接口逆向工程，包装为 API 出售给多人使用，一个 20 美元/月的订阅被分割给十几人使用，边际成本极低。
- **定价套利**：利用 Coding Plan 与 API 之间的价差。举例而言，某平台 Coding Plan 包含 100 万 Token 免费额度，运营者购买 100 份获得 1 亿 Token，以 0.1 元/万 Token 价格转售。
- **模型降级替换**：用户支付高阶模型的费用，实际调用的可能是国产小参数模型，成本相差数十倍。

二. API 中转站经营者的法律风险层次

从现有案例和法律规定出发，API 中转站经营者的法律风险可分为三个层次：刑事犯罪、行政违法、违约责任。

(一) 刑事犯罪

- 1. 提供侵入、非法控制计算机信息系统程序、工具罪：**如果平台的自动化脚本为了绕过 OpenAI 的安全防护强行攻破或绕过了 Cloudflare 验证、图像验证码(CAPTCHA)等防火墙，则可能构成此罪。四川开江法院曾审结一起贩卖 VPN 翻墙链路案件，以该罪判处被告人江某有期徒刑四年六个月，并处罚金 50 万元。其内在逻辑在于：中转站提供的代理工具，使用户得以绕开官方 API 的地区限制访问措施，本质上构成对目标系统正常访问控制措施的规避，可被认定为“侵入计算机信息系统”的工具。
- 2. 非法经营罪：**在开篇提及的案例中，上海公安机关以涉嫌“非法经营罪”对该中转站站长采取了刑事拘留的强制措施。该罪名此前在 VPN 翻墙案件中被广泛适用，即在未取得增值电信业务经营许可证的情况下，长期、大规模地以盈利为目的提供跨境电信服务，则构成“非法经营罪”的客观要件。API 中转站同样涉及未经许可从事电信业务经营，且还存在违法提供生成式人工智能服务、数据违法跨境行为，存在被适用该罪名的风险。根据《最高人民法院、公安部关于公安机关管辖的刑事案件立案追诉标准的规定(二)》第七十九条，个人涉及非法经营的，经营数额在五万元以上，或者违法所得数额在一万元以上的，应予立案追诉。
- 3. 侵犯公民个人信息罪：**用户通过 API 中转站提交的每一条提问，都有可能包含个人信息。若中转站将用户数据收集、倒卖，或未经申报将个人信息传输至境外，则直接触犯本罪。确有实测发现，部分中转站存在恶意代码注入、窃取云凭证、盗取加密资产等行为。地下网关常常将用户聊天日志打包，转手卖给急需真实人类语料来训练本地大模型的 AI 初创企业。
- 4. 其他罪名：**此外，如通过盗刷他人信用卡获取 API 额度、使用伪造身份信息批量注册账号，还可能触犯信用卡诈骗罪或伪造身份证件罪。

(二) 行政违法

- 1. 非法经营行为：**未取得电信业务经营许可证从事电信业务经营，依据《电信条例》可能面临没收违法所得并处 3 至 5 倍罚款；无违法所得的，则处 10 万元以上 100 万元以下罚款，情节严重者责令停业整顿。使用未备案向公众提供生成式人工智能服务的，违反了《生成式人工智能服务管理暂行办法》，情节严重者可责令暂停提供相关服务。
- 2. 跨境联网违规处罚：**根据《计算机信息网络国际联网管理暂行规定》，使用未经批准的信道实现跨境联网的，由公安机关给予警告、责令停止联网，可并处 15,000 元以下罚款。
- 3. 数据跨境违规处罚：**未依法进行数据出境安全评估即向境外传输个人信息，依据《数据安全法》第 46 条，最高可处 1000 万元以下罚款，并可责令暂停相关业务、停业整顿、吊销相关业务许可证或营业执照。
- 4. 税务行政处罚：**通过支付宝/微信私账收款的经营者的普遍存在偷逃税款问题，面临补缴税款、加收滞纳金及罚款。

(三) 违约责任

API 中转站通过逆向工程将网页接口包装为 API，或通过批量注册账号获取免费额度转售，本质上是违反平台服务协议的违约行为。官方平台一旦检测到此类行为，可依据用户协议注销账号、没收剩余额度、主张违约赔偿。2026 年 1 月，Anthropic 大规模对中转商发起围剿——不再封禁 IP，而是直接识别 TLS 指纹及行为模式，表明官方已从技术层面系统性地打击中转行为。

三. 个人与企业使用境外 AI 的合规路径

API 中转站的经营者面临刑事追诉，但境外 AI 服务本身并非绝对的违禁品。关键在于“如何使用”。

(一) 个人消费者的三条路径

路径一：官方直连(高法律风险)

技术上需使用 VPN 翻墙直接访问境外大模型。根据《计算机信息网络国际联网管理暂行规定》，任何单位和个人不得自行建立或者使用其他信道进行国际联网。个人使用 VPN 访问境外互联网(俗称“翻墙”)本身即构成行政违法，由公安机关责令停止联网，给予警告，可并处 15000 元以下罚款。

路径二：通过 API 中转站(高数据风险)

用户明知系违规渠道仍使用，可能被认定为共同违法，但普通消费者个人使用通常不构成刑事犯罪。更大的风险在于数据安全：用户输入可能被倒卖，预充值余额可能因平台跑路而损失，模型可能被降级，甚至被植入恶意代码。API 中转站的使用风险远不止于法律层面，数据安全与财产安全风险同样显著。

路径三：通过合规境内代理服务(推荐)

选择已取得相关资质的境内服务商，使用前应审查服务商是否已合法接入海外大模型并提供稳定访问。该路径是目前对个人用户最为稳妥的选择。

(二) 企业用户的合规要求

企业使用境外 AI 的合规要求远比个人复杂。建议企业在使用境外 AI 前建立完整的合规体系：

1. **选择合规服务商。** 优先选用已建立数据安全体系、通过等保测评的服务商。选择时应重点审查服务商的 API Key 来源、资质合规性、数据处理透明度、服务等级协议及法律责任归属。
2. **评估是否需要完成数据出境合规监管程序。** 根据《数据出境安全评估办法》《个人信息出

境标准合同办法》《促进和规范数据跨境流动规定》，非关基单位向境外提供个人信息，年度累计超过 100 万人以上非敏感个人信息/10 万人以上敏感个人信息的，必须通过国家网信部门组织的安全评估；年度累计出境 10 万-100 万非个人信息/10 万人以下敏感个人信息的，则可选择订立标准合同或通过保护认证。同时应建立数据分类分级、出境风险自评估及数据出境全流程管理制度。

因此，除非明确要求终端用户不上传个人信息，应落实以上跨境相关合规要求。

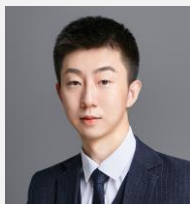
3. **注意数据输入安全。**建立内部 AI 使用管理制度，严禁将商业秘密、核心代码、未公开客户信息等敏感数据通过未经合规评估的渠道输入境外 AI，否则可能构成泄露商业秘密，承担民事赔偿甚至刑事责任。
4. **建立内部数据合规制度。**参照《生成式人工智能服务管理暂行办法》《网络信息内容生态治理规定》等法规，建立涵盖内容治理、个人信息保护、数据跨境合规、算法安全、行业专项合规等全链路的内容管理制度，对境外 AI 进行同样标准的审核和管理。
5. **采用合法合规的信道进行跨境联网。**优先选用三大运营商的跨境联网线路。如果需要使用其他供应商的线路，应要求其提供三大运营商的授权许可或与其的合作合同。

结语

API 中转站业务正从“灰色套利”走向“刑事追诉”。上海站长的 37 日拘留经历已成为行业首例警示性事件。可以预见，更多类似案件或将进入司法程序。

但用户无须过度恐慌。当前刑事打击的核心对象是**违法经营者与规模化商业行为**，规制的是违反中国生成式人工智能服务安全性、合规性方面要求的大模型桥接行为。对个人用户而言，真正需要警惕的不是法律责任，而是数据安全、账户安全与资金安全——通过非正规渠道使用境外 AI，用户无从知晓自身对话记录是否被截留、预付款项是否安全。对企业用户而言，选择合规渠道、建立完善的数据合规体系，方为稳健之策。

如您希望就相关问题进一步交流，请联系：



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com



邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2026