通力合规评论 —— 2025 年 4 月
拥抱 AI，你知道怎样才合规吗?

随着这两年 AI 技术突飞猛进的发展，AI 产品和工具早已脱离了“尝鲜”的阶段，而成为可以切切实实提升企业效率的生产力工具。但大部分企业在评估和部署 AI 产品时，面对纷繁复杂的 AI 法律和监管要求，往往瞻前顾后，既想拥抱 AI，又担心使用 AI 带来的法律风险。

因此，我们结合近期客户集中提出的一些有关于 AI 的合规问题，来给大家划一划，使用 AI 的合规边界。

1. 哪些“AI”落入中国的监管范围?

“AI”(人工智能)是一个非常宽泛的概念，它指的是通过计算机程序或机器来模拟、实现人类智能的技术和方法。但是并非所有符合上述定义的 AI 都落入中国法律的监管。

目前，中国有关 AI 的法律法规主要有以下几部:

- **《互联网信息服务算法推荐管理规定》(“算法推荐规定”)**是规范**算法推荐技术**的法规，算法推荐技术包括生成合成类、个性化推送类、排序精选类、检索过滤类、调度决策类等等。因此，使用上述算法的 AI 产品需要遵守《算法推荐规定》的要求

- **《互联网信息服务深度合成管理规定》(“深度合成规定”)**是规范利用**生成合成类算法**制作文本、图像、音视频及虚拟场景的技术的法规。结合《算法推荐规定》，可以看出深度合成技术是算法推荐技术的一个子集。因此，使用深度学习、虚拟现实等生成合成类算法不仅需要遵守《深度合成规定》，而且需要遵守《算法推荐规定》，而使用深度合成技术的 AI 产品也同时受到上述两部法规的规制

可以看出，上述两部法律主要规制的是特定的算法(如推荐算法、生成合成算法)，而不直接针对所有 AI 产品，只有使用到相应算法的 AI 产品才会落入上述法规的范围。而算法与 AI 的关系，简单来说可以理解为，算法是构建 AI 产品的基础，AI 产品的实现通常依赖于一种或多种算法。因此，**规制特定算法的法律不适用于未应用该算法的 AI，而规制 AI 的法律一定涉及对其所应用算法的规制**。

而以下几部，则是对 AI 本身进行规制的法规:

- **《生成式人工智能服务管理暂行办法》(“人工智能办法”)**是规制具有内容生成能力的模型及相关技术的法规。利用生成式人工智能技术生成文本、图片、音频、视频等内容的 AI 产品均受到《人工智能办法》的规制。

- **《人工智能生成合成内容标识办法》**要求对 AI 生成内容添加显式(文字、语音提示)或隐式(元数据、数字水印)标识，便于溯源和防止虚假信息传播

- **《科技伦理审查办法(试行)》(“伦理审查办法”)**要求对以人为研究参与者的科技活动(例如分析、处理个人信息的 AI 产品)进行科技伦理审查

通过对上述法律的总结，不难看出目前中国的 AI 法律体系下，主要规制的是面向公众提供服务的生成式 AI，并且将合规义务主要客以 AI 产品的开发者和提供者。而绝大多数企业只是 AI 产品使用者，那么是不是 AI 产品的使用者在中国法下就可以“随心所欲”了呢?答案当然是否定的。下文中，我们主要以 AI 产品使用者的视角，为大家梳理相关的合规风险和合规义务。

2. 中国境内企业是否可以使用境外 AI 产品?

许多跨国公司的中国实体，由于总部统一要求的原因，需要使用境外的 AI 产品，例如 ChatGPT、CoPilot 等等。但问题在于，这些境外 AI 产品往往像 Google、LinkedIn 等境外服务一样，要么不向中国境内的用户开放，要么是被中国的防火墙所屏蔽，所以需要使用 VPN 等技术手段，才能够在中国境内访问。很多企业关心的是，通过这样的方式在中国境内使用境外 AI 产品，是合规的吗?

- **使用境外 AI 产品本身并不违法:** 首先需要明确的是，使用 AI 产品，包括使用境外 AI 产品，本身并不违反任何中国法律。境内企业在履行了其他中国法律要求的合规义务的前提下，完全可以合法使用境外的 AI 产品
- **跨境联网的合规性:** 大部分境外 AI 产品需要使用 VPN 才能访问，而包括 VPN 在内的跨境联网行为，是受到中国法律规制的。根据中国法律，国际联网必须通过中国政府批准的国际通信出入口局进行，任何绕开国际通信出入口局进行国际联网的行为均属违法。因此，在选择 VPN 等跨境联网服务的供应商时，企业有必要关注这些供应商的跨境链路是否符合中国法律的规定，否则轻则可能会因为供应商违法被取缔，面临跨境联网服务无法使用的境地，重则可能因为违法进行跨境联网而承担法律责任。通常而言，选择中国三大电信运营商(移动、电信、联通)以及他们的授权服务提供商或合作伙伴提供的跨境联网服务是符合中国法律的规定的
- **内容的合规性:** 中国法律禁止利用国际联网行为从事危害国家安全、泄露国家秘密的行为，禁止制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情信息。如果使用境外 AI 产品，无法保证相关 AI 产品不产生违反中国法律的内容。因此，建议使用境外 AI 产品的境内企业建立内部制度，规范员工使用境外 AI 产品的行为，这可以在一定程度上避免企业因为员工违法使用境外 AI 产品而承担责任; 此外，还可以考虑使用技术手段，选择境内的供应商，对于境外 AI 产品的输出内容提供过滤服务

3. 选择 AI 产品时，有哪些审查要点?

从 AI 产品使用者的角度而言，在考虑接入 AI 大模型或者使用第三方 AI 时，最重要的是需要确保 AI 模型或产品的合规性，即确保 AI 产品提供方及 AI 产品满足中国法律下的合规要求。具体而言，有以下重点内容:

- **是否完成大模型备案/登记**：《人工智能办法》要求具有舆论属性或社会动员能力的、面向境内公众提供生成式 AI 服务的主体进行生成式 AI 服务的安全评估，即“大模型备案”；而对于调用第三方大模型提供生成式 AI 服务的主体，在其所调用的第三方大模型已完成备案的前提下，可以在完成登记后，上线提供服务
- **是否完成算法备案：**《算法推荐规定》及《深度合成规定》均规定具有舆论属性或社会动员能力的、面向境内公众提供算法推荐服务或深度合成服务的服务提供者进行算法备案
- **是否具有增值电信许可：**基于具体的 AI 服务内容和业态，相关的 AI 服务有可能构成增值电信业务，从而需要根据法律的规定取得增值电信经营许可。例如，利用生成式 AI 提供互联网信息服务，可能需要取得 ICP 证；其他可能涉及的电信业务许可包括但不限于 EDI 证、IDC 证、ISP 证、SP 证等
- **是否完成科技伦理审查：**对于涉及科技伦理敏感领域的生成式 AI 服务，应关注其 AI 产品是否根据《伦理审查办法》及《算法推荐规定》《深度合成规定》完成了科技伦理审查

4. 使用 AI，需要注意哪些合规问题？

- **开放使用 AI 的人员范围和产品范围：**使用 AI 产品(尤其是境外 AI 产品)可能会给企业带来额外的法律风险，因此，部分跨国企业对于使用 AI 产品的人员范围持谨慎态度，例如，仅将使用 AI 产品的权限开放给高级管理人员，或者根据工作职责确有需要使用 AI 产品的员工；AI 产品范围方面，企业需要考虑是否通过建立 AI 产品的“白名单”的方式来限制员工可使用 AI 产品的范围，并限制员工将未经允许的 AI 产品用于工作目的、在工作设备上安装或使用未经允许的 AI 产品，或者使用企业的网络和 IT 环境使用未经允许的 AI 范围

- **知识产权合规：**使用 AI 产品生成的文字、视频、图像等成果，如果与用于生成该内容的原始内容存在实质性相似，可能侵犯原作品的“复制权”和“信息网络传播权”，而如果 AI 产品在保留作品基础表达的前提下形成了具有独创性的新的表达，则可能侵犯原作品的“改编权”。而对于 AI 生成作品侵权的行为，到底是由 AI 产品的提供者，还是 AI 产品的使用者来承担责任，或者两者共同承担责任，目前中国司法实践并没有一个明确的结论。因此，企业应该谨慎使用 AI 产品形成的作品，尤其是如果需要将 AI 的作品对外提供或发布的，建议在内部建立事前的**AI 著作权侵权审查机制**，防止因为 AI 的著作权侵权而承担责任

- **内容合规：**通常而言，境内的 AI 大模型提供方都对其 AI 产品生成的内容设置了审查机制，可以避免生成在中国法律或政治环境下的敏感内容；但境外的 AI 产品普遍没有这样的机制。建议参考第 2 点中列出的内容合规要点，采用制度或技术措施，防止内容合规风险。此外，除了法律层面的内容合规风险外，企业还需要防止企业层面的内容合规风险，例如，AI 产品可能会产生侵犯企业商业秘密或者有损企业名誉的内容

- **个人信息保护：**如果员工使用 AI 产品，随意对企业收集、形成的个人信息用进行处理和分析(例如，对于企业收集的消费者个人信息进行跨境传输，或者将客户的个人信息输入 AI 产品进行分析)，即使此前企业收集相关个人信息的行为是合规的，员工的该等处理也很有可能超出此前企

业获得的个人信息主体的同意范围，从而构成违法处理个人信息，导致企业承担相应的法律责任。因此，需要制定相应的内部政策，来规范员工使用 AI 产品处理个人信息的行为。此外，建议将 AI 产品可能涉及的个人信息处理纳入企业的**个人信息保护影响评估**流程，确保 AI 产品的使用不会对个人信息权益造成不利影响

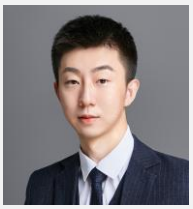
如果企业使用的是 SaaS 类型(即非本地部署)的 AI 产品，还需要额外考虑以下合规问题:

- **商业秘密保护:** 对于非本地部署的 AI 产品而言，员工将其用于日常工作的一个潜在风险是，员工需要将其日常工作接触的企业自身乃至第三方的数据和信息提供给 AI 产品，而这将会导致企业的数据被传输至 AI 产品提供方(还可能包括 AI 产品服务方使用的供应商)的服务器，从而导致企业的敏感数据和商业秘密可能被第三方获取，造成商业秘密的泄露。因此，建议在企业**数据分类分级工作**的基础上，明确哪些数据和信息构成企业的商业秘密，并对员工在 AI 工具中使用这些数据和信息做出限制或设置审批流程

如果企业将相关 AI 产品开放给外部人员/公众使用的，企业自身角色将从单纯的“使用者”转变为“AI 服务提供者”，除确保 AI 产品本身合规之外，企业也需要评估是否需要履行本文第 3 点所列举的备案/登记、电信业务许可、科技伦理审查等义务。

我们希望本期合规评论能帮助您更好地理解中国法律下使用 AI 的合规要求。如果您希望了解更多有关 AI 合规的内容，或者希望了解我们网安数据领域其他法律服务，欢迎与我们取得联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



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

往期文章:

AI 也有“署名权”了？简评《人工智能生成合成内容标识办法》
美国对华限制政策新发展——人工智能篇/生物医药篇
简评《生成式人工智能服务管理办法(征求意见稿)》七大问题
隐私计算技术对数据开发利用的突破与限制
AI 不是你想买，想买就能买——从出境合规视角看中美人工智能技术监管
算法推荐 深度合成 生成式 AI？傻傻分不清楚
利好 AIGC 行业？——AIGC 著作权第一案评析

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	北京	深圳
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	伦敦	
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	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