ChatGPT 花式整活进行时：边界何在?

作者：潘永建 | 朱晓阳 | 王雪莹 | 吴若蘅

一. 引言

如果你是一个追求时髦的人，最近你一定“玩”过 ChatGPT。你用 ChatGPT 干过什么?写论文，还是写代码、做图表、想创意?亦或是单纯的聊天解闷?当你在与 ChatGPT 互动时，你是否想过，如果不加注意，小小的 ChatGPT 聊天窗口背后可能是一个巨大的合规黑洞?在前文《狂飙的 ChatGPT，合规“缰绳”何在?》中，我们结合《互联网信息服务深度合成管理规定》及我国其他网络安全与数据合规领域的法律法规，从 ChatGPT 类产品开发运营者的角度探讨了其潜在风险与合规边界，而在本文中，我们将聚焦于广大用户群体，对企业及个人在使用该类产品时的合规风险与义务进行提示。

二. 典型法律风险及风险防范建议

(一) ChatGPT 类产品通用合规风险及建议

1. 商业秘密泄露风险

如我们在前文中所述，ChatGPT 类产品的完善需要大量的数据输入来对 AI 进行训练，这些数据中，OpenAI 等产品开发方自行收集并“喂”给 ChatGPT 的仅仅是一部分，大量的数据其实是在用户使用 ChatGPT 的过程中提供的。当用户使用 ChatGPT 类产品并提交信息时，该信息便会作为训练数据用于生成为其他用户提供的回答、完成请求等。在此过程中，如果企业或者企业员工提供了企业的敏感信息，很有可能因此导致企业商业秘密或其他敏感信息的泄露。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

商业秘密(Trade Secrets)，一般是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。作为企业的重要财产性权利，它是企业的竞争力之所系，商业秘密的保护将对企业的发展至关重要。因此，企业有必要采取“必要的保密措施”来保证商业秘密在合理的条件下不至于被泄露，满足其“秘密性”要求。相反，如果在企业未对员工进行任何约束的情况下员工将保密数据主动提供给 ChatGPT，可能会被视为企业自行放弃了商业秘密的秘密性及未对商业秘密采取必要的保护措施。

如果企业在开展业务过程中需要员工使用 ChatGPT 的，对于 ChatGPT 类产品可能存在的商业泄露风险，我们建议公司在建立内部保密规章制度、与员工签订保密协议或提出保密要求时，制定相关规则禁止或限制员工向 ChatGPT 上传可能涉及公司商业秘密的相关信息。同时，需要向员工事先明确公司商业秘密的类型和范围，必要时要求员工在使用 ChatGPT 类产品时要将提交的信息事先提交法务/合规/知识产权部门进行审查，并且明确违反该等规定需要承担的相应法律责任。

2. 内容合规风险

ChatGPT 类产品生成的信息包罗万象，但却并非都是真理。使用者还应当注意 ChatGPT 类产品生成的包含违法、违规信息的答复内容，特别是在答案可能构成违法违规信息的前提下对其进行传播的法律后果。

相关研究表明，比起“冷冰冰的搜索引擎”，人类天生更容易相信从“更具人情味”的聊天机器人处获取的答案[1]。虽然该类产品在开发前通常需要接受严格测试以减少“出错”概率，但其作用和实际效果也毕竟有限。更与传统搜索引擎不同的是，聊天机器人在与用户交流的过程中并不需要向用户展示一连串的链接，且由用户自行决定信任与选择哪些信息，其自动化决策的过程和运作方式是缺乏透明度的[2]。因此，如果用户盲目地信任 AI 自动生成的答案或产出成果并进行传播，将会十分危险。

例如，根据我国《治安管理处罚法》和《刑法》的相关规定，散布谣言，在信息网络或以其他方式谎报险情、疫情、警情等涉及公共利益情况的，将可能受到拘留、罚款等行政处罚，严重可招致刑事责任。目前，网安数据的监管部门对此也有所关注，并特别指出，“一旦 ChatGPT 被不法分子利用，将成为成本与门槛极低、效率与产出极高、可信度极强的造谣工具”。比如近日网上传播的一则新闻，制造出“杭州决定取消限行”的吸睛话题而导致许多人信以为真，但最终该新闻被证实为 ChatGPT 所写[3]。

[1] Nature Portfolio, 《ChatGPT 颠覆传统搜索引擎，它的回答能信几分?》, https://mp.weixin.qq.com/s/i31vEQgPsrrVMLj5VkBivw

[2] Philipp Hacker, Andreas Engel, Marco Mauer, *Regulating ChatGPT and other Large Generative AI Models,* https://arxiv.org/abs/2302.02337

[3] 西藏网警、网信内蒙古等, 《ChatGPT 如何依法合规正确使用?》, https://mp.weixin.qq.com/s/M3pc0DW2J88ZqEX-Ij5Gdw, 原载于人民邮电报

针对 ChatGPT 这一特点，我们建议使用者需谨慎对待 ChatGPT 答复内容或其他生成成果，如果需要将 ChatGPT 类产品生成的内容对外提供(尤其是公开发布)的，建议企业提前发布内容合规的指南或者手册给员工参考，对于重大的内容，还应当在对外提供/发布前由法务/合规部门进行审核，否则一旦成为违法违规信息的传播者，企业也可能为此承担法律责任。此外，企业还应注意加强员工培训、增强其风险意识，避免不必要的商誉损失。

(二) 境外 ChatGPT 类产品使用的合规建议

除上述提及的常规风险以外，如在我国境内使用境外部署的 ChatGPT 类产品，还会有一些额外的合规风险考量。我们提示用户应对向其提供个人信息、敏感个人信息及重要数据等所涉及的数据出境风险、跨境联网以及购买、租用账号风险等予以关注。重点提示如下:

1. 数据出境风险

以 ChatGPT 为例，由于其服务器部署在境外，当用户在聊天界面提问时输入的信息包含公司在境内运营过程中收集和产生的数据时，企业将涉及“向境外提供”数据，或存在该等数据能够被境外机构、组织或者个人“访问或调用”的法定数据出境情形。

为此，针对每一类数据的特别规定，我们提示以下风险点并提出相应的合规建议:

	数据类型/数量	合规风险	合规建议
1.	国家秘密	本地化存储，出境须经过严格审批	仅限具有严格保密义务的必要范围的员工知悉，并采取严格安全保障措施，如禁止员工在使用 ChatGPT 时输入相关数据
2.	• 重要数据关键信息基础设施运营者收集和产生的个人信息 • 处理人数达到网信办规定数量的个人信息	原则上本地化存储，传输至境外须经过网信办的出境安全评估	本地存储相关数据，同时禁止员工在使用 ChatGPT 时输入相关数据，相关规定纳入员工管理考核、内部风控建设体系
3.	特定行业数据: • 人口健康信息 • 健康医疗大数据 • 人类遗传资源信息 • 未公开的国家基础地理信息	仅能本地化存储，不得传输至境外并存储	本地存储相关数据，同时禁止员工在使用 ChatGPT 时输入相关数据，相关规定纳入员工管理考核、内部风控建设体系
4.	个人信息	(1) 就个人信息出境的情况告知相关个人，并取得其单独同意;	建议企业采取禁止性或限制性手段避免员工在使用 ChatGPT 时披露个人信息，

		(2) 出境前进行个人信息保护影响评估; (3) 需要进行出境安全评估申报: a. 向境外提供重要数据; b. 属于关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者; c. 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息	以防止此类出境的情境和数量不可控
5.	其他未受特别规制的数据	仍存在造成企业商业秘密外泄的风险	建议企业制定相关规则禁止或限制员工向 ChatGPT 上传可能涉及公司商业秘密的相关信息。 同时，向员工事先明确公司商业秘密的类型和范围，必要时要求员工在使用 ChatGPT 类产品时要将提交的信息事先提交法务/合规/知识产权部门进行审查，并且明确以及违反该等规定规则需要承担的法律责任。

2. 买卖、租用账号风险

目前，ChatGPT 并未开放中国用户使用、无法用国内手机号进行注册，这一限制也催生了一项新的“生意”，即一些商家自行搭建或使用 VPN，并通过闲鱼等网络平台以出售和出租账号，代注册、包月访问 ChatGPT 账号等方式赚取差价。

虽然 ChatGPT 本身对是否禁止买卖、租用账号暂无规定，但上述商家以营利为目的、在未办理国家相关行政许可的前提下搭建或使用 VPN 进行注册账号并擅自经营买卖国外账号的行为，可能涉嫌非法经营[4]。此外，根据《互联网用户公众账号信息服务管理规定》，公众账号生产运营者不得以虚假身份信息进行注册，因此商家也可能受到行政处罚或承担刑事责任。

购买账号的使用者也将为此面临一定风险。由于已涉嫌非法经营，该等商品不仅没有售后服务保障、无法维护消费者的合法权益，而且账号本身还可能被卖家收回。如果遇到一号多售的情况，不但影响用户的使用体验，还很有可能造成个人信息和其他数据的泄露。

[4] 《ChatGPT 大火 广东消委会提醒：代注册账号涉嫌非法经营》，http://fashion.ce.cn/news/202303/02/t20230302_38421377.shtml

3. 跨境联网风险

在注册和使用阶段，用户还需将自己的国内 IP 地址切换至境外方可正常访问。如果企业通过自建信道等违规方式实现访问境外网站的，可能会因此受到处罚。即使是合规搭建的跨境联网架构，如果员工通过公司专线等向 ChatGPT 类产品传输或者获取违法、违规的信息，不仅员工个人可能会受到行政处罚或承担包括利用信息网络传播违法犯罪活动信息罪在内的刑事责任，也会给公司带来名誉损失。

此外，如果员工在企业内网中使用自己购买的 VPN 跨境联网，由于其获取的 VPN 本身可能属于违反工信部的规定未经批准“自行建立或租用专线(含虚拟专用网络 VPN)开展跨境经营活动”的情形，员工作为使用者也可能会因此受到行政处罚(此前已有多起 VPN 使用者被处罚的案例)。此外，与购买 ChatGPT 账号的风险类似，也将面临没有售后服务保障、无法维护自身合法权益的困境，甚至在此过程中泄露个人信息，并对企业内网的可见性产生风险和威胁等[5]。

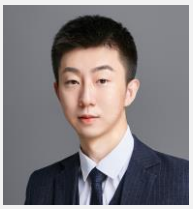
三. 结语

ChatGPT 等新型产品的诞生无疑为企业在新形势下满足我国网安数据法的合规监管要求提出了新的挑战。无论是作为产品的开发者、运营者的从业人员，还是想要使用该类产品的企业用户，均需关注自身的合规风险与义务，我们也将对相关技术和该领域的法律法规发展持续关注。

[5] 《在企业内网中使用个人 VPN 的潜在风险》, https://mp.weixin.qq.com/s/tj-AbAeyAHt-p4kWwNMSAg

如您希望就相关问题进一步交流，请联系：

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



朱晓阳
+86 21 3135 8683
nigel.zhu@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	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