

类 ChatGPT 应用的法律风险与合规建议

文 婷

摘 要：2022 年 11 月 ChatGPT 发布后，在全世界迅速引起一股人工智能关注及应用的浪潮，在 ChatGPT 用户及使用量暴增的同时，国内科技公司亦加紧步伐布局类 ChatGPT 应用。国内用户（不含港澳台）在使用 OpenAI 公司研发运营的 ChatGPT 时，不仅涉及“翻墙”的行政违法行为，还涉及数据出入境的合规问题。此外，对于国内（不含港澳台）的类 ChatGPT 应用，运营方需要取得增值电信业务经营许可证及其他依据法律法规必要取得的合规资质后方可提供类 ChatGPT 服务，同时数据合规及安全问题仍然是类 ChatGPT 应用需要关注的重点法律问题。此外，知识产权侵权风险、因类 ChatGPT 输出回答错误虚假而导致他人遭受损害的法律风险、类 ChatGPT 被犯罪利用而导致运营公司可能遭受的民事或刑事责任、类 ChatGPT 的算法与伦理风险等均是类 ChatGPT 运营公司需要关注的法律问题。

关键词：人工智能；数据合规；知识产权；犯罪利用

中图分类号：TP18；D92 **文献标识码：**A **文章编号：**1673-5706（2023）02-0040-06

2023 年“ChatGPT”火爆网络，成为最引人关注的名词及应用之一。根据 UBS 发布的研究报告显示，ChatGPT 在 2023 年 1 月份的活跃用户数已达 1 亿，成为目前史上用户数增长最快的消费者应用。根据 Similar Web 的数据，1 月份平均每天有超过 1300 万名独立访问者使用 ChatGPT。与此同时，国内外科技公司纷纷布局类 ChatGPT 应用，其中包括微软、谷歌、百度、阿里巴巴、腾讯、360、字节跳动、科大讯飞、京东、网易、百融云创等科技巨头，其主要应用于智能搜索、智能地图、智能办公、智能营销、智能客服、智能城市、智能教育等领域及场景。ChatGPT 及类 ChatGPT 应用火爆全网的同时，参与者、运营方更需要了解其涉及的合规问题及法律风险。本文拟主要从三个角度剖析类 ChatGPT（含 ChatGPT）及其涉及

的法律问题，并提供相应的建议。

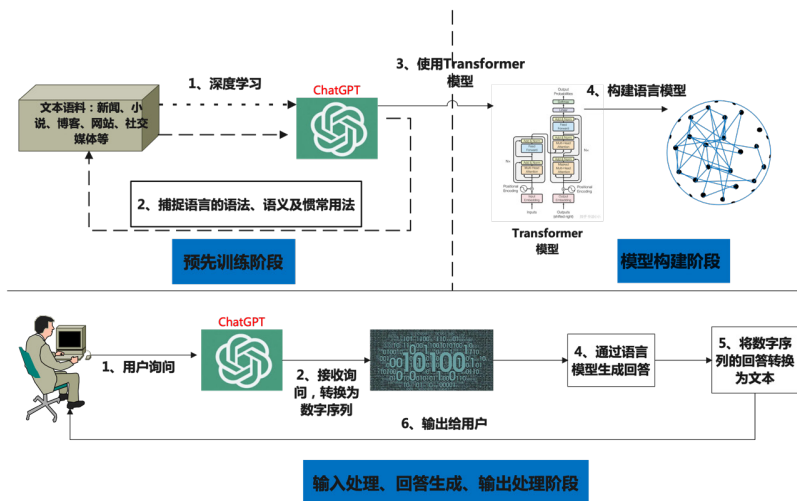
一、什么是 ChatGPT

ChatGPT 是由人工智能研究实验室 OpenAI（OpenAI 于 2015 年由马斯克、美国创业孵化器 Y Combinator 总裁阿尔特曼、全球在线支付平台 PayPal 联合创始人彼得·蒂尔等硅谷科技大亨创立）在 2022 年 11 月 30 号发布的全新聊天机器人模型，一款人工智能技术驱动的自然语言处理工具。ChatGPT 能学习和理解人类的语言，像人类一样进行聊天交流，并能根据上下文与人类进行互动。

但如果仅仅将 ChatGPT 理解为聊天机器人就过于狭隘了，ChatGPT 被大量运用于各类应用场景，如智能客服，不仅能回答客户的问题，还能依据客户的意图和情绪，提供交互式、人性化、24 小时不间断的服务；文本生成，可以自动生成

各种类型的文本，包括新闻报道、小说、演讲稿、诗歌、散文、论文甚至法律意见书等；语音识别与生成，可以智能识别语音并做出相应的回应；数据分析与营销决策支持，利用 ChatGPT 可以进行数据分析和挖掘，并根据数据分析和挖掘的结果，生成数据可视化报告，为营销决策提供支持。ChatGPT 亦被广泛应用于各行各业，如教育行业、金融行业、医疗行业、传媒行业等。

ChatGPT 需要大量的数据形成训练集进行模型训练，通过对训练集的深度学习掌握人类语言的语法、语义及使用习惯，并在此基础上，通过使用 Transformer 模型来构建 ChatGPT 自身的语言模型，再通过语言模型处理用户的输入及回答的输出（见下图）。



ChatGPT 工作原理示意图

二、在国内（不含港澳台）使用 ChatGPT 涉及的法律问题及合规建议

目前 OpenAI 没有在中国大陆提供有关 ChatGPT 的服务，也没有设立相应的公司运营 ChatGPT。在中国大陆地区使用 ChatGPT 服务，或需通过“翻墙”访问，或使用“中间商”（即

先取得 ChatGPT 官方接口，再提供给国内用户使用的商家）提供的 ChatGPT 服务。在国内（不含港澳台）使用 ChatGPT 服务，最常见的法律问题便是“翻墙”违规及数据跨境问题。

（一）“翻墙”问题

依据《中华人民共和国计算机信息网络国际联网管理暂行规定》第六条：“计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出入口信道。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。”同时，第十四条规定：“违反本规定第六条、第八条和第十条的规定的，由公安机关责令停止联网，给予警告，可以并处 15000 元以下的罚款；

有违法所得的，没收违法所得。”

因此，通过“翻墙”软件访问 ChatGPT 属于行政违规行为，可能被处以罚款及没收违法所得。

（二）数据跨境合规问题

根据 ChatGPT 的工作原理，用户在输入端口提出问题后，该问题信息会被传输到美国的 OpenAI 公司，ChatGPT 生成相应的回答后，该回答便会传输、反馈到用户的端口。在问答输入/输出过程中便涉及数据出境/入境的跨境问题，尤其在数据出境领域，若用户所提的问题涉及个人信息、敏感信息甚至国家安全、公共健康和安全等领域的重要数据，则存在严重的法律风险。

根据《数据出境安全评估办法》等相关法律法规，若使用 ChatGPT 导致重要数据^①出境应该向国家网信部门申报数据出境安全评估，若关键信息基础设施运营者^②使用 ChatGPT 导致个人信息数据

① 根据《金融数据安全数据安全分级指南》《信息安全技术 重要数据识别指南》，重要数据是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成危害国家安全、损害国家财产等严重后果的数据。

② 根据《关键信息基础设施确定指南》，关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

出境,或其他特定主体(处理100万人以上个人信息的数据处理者或自上年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的数据处理者)因应用/使用ChatGPT导致个人信息出境,均应向国家网信部门申报数据出境安全评估并获得准许。因此,“数据出境无小事”,尤其是掌握重要数据的企业组织或个人,大量处理个人信息、敏感信息的主体在应用/使用ChatGPT的时候更应关注数据出境的法律风险,按照法律规定获得合法准许、按照法律法规的要求规范各种流程、程序和文件后才能合规“数据出境”。否则,根据《个人信息保护法》《网络安全法》《数据安全法》《数据出境安全评估办法》等相关法律法规的规定,数据违规出境的主体可能承担的法律风险包括但不限于:被警告,被没收违法所得,根据情节轻重被处以罚款或巨额罚款,被责令暂停业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照,直接负责的主管人员和其他直接责任人员也可能处以罚款或在一定期限内禁止担任相关职务等,构成犯罪的,甚至可能被追究刑事责任。

三、在国内(不含港澳台)运营类 ChatGPT 服务涉及的法律问题及合规建议

自从ChatGPT爆火后,国内各大科技企业加速入局AIGC(人工智能自动生成内容)赛道,推出相关竞品(即类ChatGPT服务)。根据《互联网信息服务管理办法》《互联网信息服务深度合成管理规定》《互联网信息服务算法推荐管理规定》《深圳经济特区人工智能产业促进条例》《上海市促进人工智能产业发展条例》《新一代人工智能伦理规范》等相关法律法规文件,笔者认为在国内(不含港澳台)运营类ChatGPT服务涉及的法律问题及风险包括但不限于以下几类:

(一) 资质问题

根据《互联网信息服务管理办法》第四条规定,国家对经营性互联网信息服务^①实行许可制度,

对非经营性互联网信息实行服务备案制度,未取得许可或者未履行备案手续的,不得从事互联网信息服务。同时,《互联网信息服务管理办法》第七条规定:“从事经营性互联网信息服务,应当申请办理互联网信息服务增值电信业务经营许可证。”根据《中华人民共和国电信条例》的规定,未取得电信业务经营许可证,任何组织或者个人不得从事电信业务经营许可。

类ChatGPT服务属于互联网信息服务,一般会向用户收取相应的费用以维持高额的运营投入,并实现商业目的。因此,在国内(不含港澳台)运营类ChatGPT服务应取得增值电信业务经营许可证。依据《中华人民共和国电信条例》及《电信业务分类目录》的规定,电信业务分为基础电信业务和增值电信业务,其中,增值电信业务又分为两类,根据类ChatGPT服务的具体情况,建议同时取得第二类增值电信业务之B21许可证(增值电信业务经营许可证——在线数据处理与交易处理业务)、B25许可证(增值电信业务经营许可证——互联网信息服务)。如果类ChatGPT输出的内容涉及金融、医疗等特殊领域,则根据该特殊领域监管的规定,类ChatGPT运营主体亦可能被要求取得相应的资质。如类ChatGPT输出的内容如果涉及证券投资分析、预测或者建议,并且运营方收取相关费用,则运营方应取得中国证监会许可的证券投资咨询资质。此外,若作为类ChatGPT技术方与银行、保险等金融机构合作提供类“ChatGPT”应用服务,则可能被视作信息科技外包服务商,按照《银行保险机构信息科技外包风险监管办法》,该外包服务商需满足技术、行业经验、信息安全保障能力、持续经营能力等各方面的合规要求及“准入”资质。笔者认为类ChatGPT一定程度上具有舆论属性或者社会动员能力,从合规角度来看,建议根据《互联网信息服务算法推荐管理规定》ChatGPT应进行算法备案^②。同时,若类ChatGPT应用提供的服务

^① 根据《互联网信息服务管理办法》,经营性互联网信息服务是指通过互联网向上网用户有偿提供信息或者网页等制作服务活动。

^② 《互联网信息服务算法推荐管理规定》第二十四条规定,具有舆论属性或者社会动员能力的算法推荐服务提供者应当在提供服务之日起十个工作日内通过互联网信息服务算法备案系统填报服务提供者的名称、服务形式、应用领域、算法类型、算法自评估报告、拟公示内容等信息,履行备案手续。

涉及网络音乐、网络动漫、网络表演等领域，应具备相应网络文化经营许可证；若类 ChatGPT 应用提供的服务涉及网络出版服务、网络视听节目服务等领域，还应具备网络出版服务许可证、信息网络传播视听节目许可证等资质。

（二）数据合规问题

类 ChatGPT 的数据合规问题贯穿于数据收集、存储、使用、加工、传输、提供等各个环节。

类 ChatGPT 收集数据涉及训练集中用于训练的数据、用户输入的内容等。对于训练集中的数据，如果来源于公开信息，需要特别注意其中是否涉及个人信息。根据《中华人民共和国民法典》第 1035 条、第 1036 条以及《个人信息保护法》第 27 条的规定，若涉及公开信息中的个人信息，如果个人通过任何方式明确表示拒绝，则不可对该个人信息进行收集和抓取。另外如果收集、抓取已公开的个人信息对个人权益有重大影响，也不可径行抓取，而应取得个人同意。对于用户输入的内容，也可能涉及个人信息，依据《个人信息保护法》《数据安全法》等相关法律法规的规定，类 ChatGPT 运营方应取得个人的授权同意，明确收集个人信息的目的、方式、范围，这就要求类 ChatGPT 在用户注册的时候以适当的方式签署《用户协议》及规范的《隐私政策》。此外，类 ChatGPT 运营方应加强敏感信息的自动识别技术，在识别到生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感信息，以及不满十四周岁未成年人的个人信息时，应采取弹窗等醒目方式单独告知个人处理该敏感信息的必要性、目的、方式和范围，以及对个人权益的影响，并取得个人的单独同意后才可收集和处理敏感信息。

类 ChatGPT 在处理相关数据的过程中，可能涉及数据泄漏的风险，用户输入内容时可能涉及个人信息、业务数据甚至商业秘密的内容，这些内容一旦泄漏可能导致严重后果。自 2023 年 1 月开始，微软与亚马逊先后禁止公司员工向 ChatGPT 发送公司机密信息，摩根大通、花旗集团和高盛集团纷纷禁用 ChatGPT，咨询公司埃森哲警告员工不要将客户信息暴露给 ChatGPT。

OpenAI 的使用条款规定了 OpenAI 对用户输入和输出内容拥有广泛使用权，用户输入、交互的内容将被纳入训练数据库，用于持续迭代训练，并用于改善 ChatGPT。OpenAI 表示“作为持续改进的一部分，当您通过我们的 API 使用 OpenAI 模型时，我们可能会使用您提供给我们数据来改进模型”。在此情况下，用户输入的信息还可能进一步被用于为其他用户提供服务，这就涉及数据共享及改变数据原使用目的的问题，根据《个人信息保护法》和 GB/T 35273-2020《信息安全技术个人信息安全规范》，接收方应当在原处理目的、方式和种类等范围内处理个人信息，若变更原先的处理目的和处理方式，应当重新取得个人同意。因此，在国内（不含港澳台）运营的类 ChatGPT 若发生个人信息被用于为其他用户提供回答输出时，如未重新取得个人授权同意，则涉及违反相关法律法规规定，应承担相应的法律责任。

对于类 ChatGPT 涉及的数据合规及数据安全的问题，除前述已提及的建议外，笔者认为要严格落实《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等相关规定，将个人信息保护作为企业合规体系建设的重要内容；遵循《个人信息保护法》《数据安全法》等的规定和配套标准，保障训练数据来源合法，收集个人信息获得有效授权及同意；将数据安全治理贯彻到类 ChatGPT 研发、运营、管理等各环节，形成长效的数据安全治理机制。具体包括：从组织建设层面，设立负责数据安全工作的组织机构和专职人员，进行明确的职责分工；在制度规范层面，制定数据安全内部管理制度和操作规程，如网络安全等级保护制度、全流程数据安全管理制度、网络安全事件应急预案、网络信息安全投诉、举报制度等；在管理流程层面，建立数据安全管理制度，通过规范化的流程确保制度规范的落实。在数据安全技术层面，使用数据加密存储技术、个人信息去标识技术、数据脱敏处理等技术保障数据安全；在人员管理与培训方面，与信息处理岗人员签署保密协议，对大量接触敏感信息的岗位进行背景调查，明确涉及信息处理岗的安全职责，安全事件处罚机制，定期（至少每年一次）

开展个人信息安全专业化培训和考核^[1]。

（三）知识产权问题

类 ChatGPT 数据挖掘和训练的过程是否需要获得相应的知识产权授权？针对这个问题，根据类 ChatGPT 的工作原理，类 ChatGPT 需要将训练集（语料库）中的内容复制到自己的数据库中（即为数据挖掘），并通过对数据库内容的深度学习进行数据训练。类 ChatGPT 在数据挖掘的过程中，若“挖掘”的内容涉及他人享有知识产权的内容，则可能涉及对他人作品的复制行为。《中华人民共和国著作权法》第二十四条规定了十三种可合理使用他人作品（可不经授权、不支付报酬）的情形，但并未将 AI 人工智能中的“文本数据挖掘”纳入到合理使用的范围。因此，笔者认为若文本数据挖掘涉及他人享有著作权的内容，则应当获得作者的授权并支付报酬。

类 ChatGPT 等人工智能生成内容是否受知识产权保护，理论界存在“肯定说”与“否定说”两种不同意见。根据《中华人民共和国著作权法实施条例》第二条：“著作权法所称作品，是指文学、艺术和科学领域内具有独创性并能以某种有形形式复制的智力成果。”目前“肯定说”与“否定说”分歧在于人工智能生成内容是否具备“独创性”，是否属于人类的智力成果。笔者认为尽管人工智能不具备独立人格，但“机器学习”的过程是一种人性化的创作行为，若人工智能生成内容的外在表现形式符合前述著作权法“作品”的构成要件，即具备“独创性”“可复制性”等，则不能将人工智能生成内容排除在“版权”保护范围之外^[2]。当然如果类 ChatGPT 输出的内容仅仅是数据的堆砌，人物、时间、地点、事件等客观事实的表达，则不具备“独创”而不受版权保护。至于权利主体的问题，依据《中华人民共和国著作权法》第十一条的规定：“著作权属于作者，创作作品的公民是作者。由法人或者其他组织主持，代表法人或者其他组织意志创作，并由法人或者其他组织承担责任的作品，法人或者其他组织视为作者。”类 ChatGPT 仅是人工智能计算机程序，因此并非我国法律上著作权享有的主体（公民、法人或者其他组织）。笔者认为类 ChatGPT

输出的内容在具备前述“作品”构成要件的情况下，著作权归属应属于“创作者”，若作品“独创性”系用户（即使用者）的智力成果，如用户输入核心要点，类 ChatGPT 仅是进行排列组合及补充修饰，则著作权应属于用户，若作品完全依赖于类 ChatGPT 平台的技术，则著作权应属于类 ChatGPT 平台公司^[3]。

针对类 ChatGPT 在输出的回答中包含第三方享有知识产权的内容，笔者认为应当获得第三方权利人的授权同意，否则可能涉及对第三方著作权中的汇编权的侵犯。

（四）虚假错误回答问题

由于类 ChatGPT 的技术并不成熟，或者用于训练的数据集存在滞后性等问题，在现阶段，类 ChatGPT 输出的内容难免出现虚假错误回答，2022 年 11 月几乎与 ChatGPT 同一时间上线的 Meta 服务科研领域的语言模型 Galactica 就因为真假答案混杂的问题，测试仅仅 3 天就被用户投诉下线。

若用户因为信赖类 ChatGPT 输出的错误信息 / 误导性内容而遭受损失，类 ChatGPT 运营者是否需要承担赔偿责任？笔者认为应从类 ChatGPT 的业务模式、盈利模式进行具体分析，若类 ChatGPT 仅提供免费的服务，并且进行充分的风险提示，则在一定程度上可以“免责”，若类 ChatGPT 提供收费服务，则其运营方承担赔偿责任的可能性较大。

（五）犯罪利用问题

自 OpenAI 2022 年 11 月发布 ChatGPT 伊始，Check Point Research（CPR）的研究人员已发现至少三起恶意利用 ChatGPT 的实例。如使用 ChatGPT 开发的 Python 信息盗取器代码，在被感染的系统上搜索和复制 Office 文档、PDF 和图片等 12 种常见文件类型并外泄；再比如用 ChatGPT 编写 Java 代码下载 PuTTY SSH 和 telnet 客户端并通过 PowerShell 在系统上秘密运行。类 ChatGPT 极易被犯罪分子利用，成为网络犯罪工具或为网络犯罪提供技术支持，如 ChatGPT 等 GPT-3 工具可帮助网络犯罪分子逼真地模拟各种社会环境，并通过心理操纵诱骗受害者泄露敏感个人信息；如网络犯罪分子利用类 ChatGPT 等工具生成极具

说服力的钓鱼电子邮件或信息实施网络诈骗。

若国内（不含港澳台）运营的类 ChatGPT 应用被犯罪分子恶意利用作为犯罪工具，其开发者、运营方是否需承担法律责任？承担何种法律责任？笔者认为作为类 ChatGPT 平台运营方，若对于被犯罪利用系“明知”而放任，则可能构成帮助信息网络犯罪活动罪（简称“帮信罪”）。刑法第二百八十七条规定：“即明知他人利用信息网络实施犯罪，为其犯罪提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助即构成帮信罪。”实践中，若平台运营被通知、被举报、被投诉类 ChatGPT 应用被利用为犯罪工具而不积极采取有关行动，阻断被犯罪利用的行为及后果，则可能被认定为“明知”而构成帮信罪，承担被处三年以下有期徒刑或者拘役，并处或者单处罚金的法律责任。

此外，不良分子可能利用 / 劫持类 ChatGPT 应用生成违法或不良信息，从而导致违法或不良信息广泛传播。对此，类 ChatGPT 运营方应主动积极履行信息网络安全管理义务，通过技术措施和人工干预的方式履行内容审核管理义务，建立健全用于识别违法和不良信息的特征库，切实防范信息网络安全风险，否则，经监管部门责令采取改正措施而拒不改正或无有效措施进行改正，平台运营方可能被追究拒不履行信息网络安全管理义务的刑事责任。

（六）算法及伦理问题

作为人工智能技术驱动的自然语言处理工具，类 ChatGPT 同样存在算法及伦理问题。类 ChatGPT 算法可能歧视某些群体或偏向某些观点，从而导致出现侵犯平等权利等情形；类 ChatGPT 的算法黑箱及算法复杂性问题，可能导致算法失控问题，类 ChatGPT 的行为可能超出人类所预设、理解、可控的范围，对人类安全产生负面影响；类 ChatGPT 应用使用不合理，包括滥用、误用、罔顾数据安全及相关法规等，则可能对社会秩序、价值等产生重大负面影响^[4]。

对此，从合规安全角度，笔者建议类 ChatGPT 运营方采取以下措施：一是提升算法透明度。进

行算法备案，借助“互联网信息服务算法备案系统”等途径公示算法的基本原理、目的意图、主要参数、主要逻辑、主要运行机制等，提升算法透明度；二是向用户（使用者）及时、准确、完整、清晰、无歧义地说明类 ChatGPT 服务的功能、局限、安全风险和可能的影响；三是从技术上不断提升类 ChatGPT 系统、服务的可解释性、可控性；四是在系统或服务中设置事故应急处置机制，包括人工紧急干预机制等。

四、结语

本文主要从法律角度阐述了在国内使用 ChatGPT 涉及的法律问题、在国内运营类 ChatGPT 服务涉及的法律问题及合规建议。ChatGPT 尚属新兴事物，科技的发展总是在不经意间改变了传统的法律关系，产生新的法律问题，但科技的发展不能离开法律的规制，建议类 ChatGPT 运营者在创新、创造的同时，更多关注由此导致的合规问题和法律风险，慎思笃行，方得长久。

参考文献：

- [1] 张莉. 数据治理与数据安全 [M]. 北京：人民邮电出版社，2019.
- [2] 郝立军，田熔榕. 论人工智能生成内容的著作权问题探究 [D]. 《上海法学研究》集刊，2022，（5）：48-56.
- [3] 孙玉荣，刘宝琪. 人工智能生成内容的著作权问题探究 [J]. 北京联合大学学报（人文社会科学版），2020，（1）：86-91.
- [4] 李伦. 数据伦理与算法伦理 [M]. 北京：科学出版社，2022.

作者：文婷，华商律师事务所高级合伙人，深圳市律师协会区块链法律专业委员会主任

责任编辑：谭博文