福建新世通律师事务所
FUJIAN NEW-STONE LAW FIRM

人工智能时代的合规挑战与法律应对

福建新世通律师事务所
陈承正 律师

陈承正 | Chen chengzheng

⭐具有中国和美国法律学习和工作经历，超过十年法律和数据双领域工作经验，致力于数字经济与人工智能领域的法律研究和实践探索。
⭐中国最早一批从事数据资产，人工智能，低空经济，可信数据空间，企业个人信息保护合规审计、企业出海及涉外投资等方面法律服务的律师。

核心职务：

- 福建省金融监督管理局企业上市辅导员
- 福建省律师协会涉外委副主任
- 福建省涉外律师人才库成员
- 福建省法学会数字法学研究会副会长
- 福建新世通律师事务所合伙人兼数字经济与人工智能专委会主任

人工智能：

- IAPP协会认证人工智能治理专家（AIGP）
- 2025年AI音乐春晚总法律顾问
- 参与20+个人工智能合规、算法备案、大模型备案、app/小程序合规项目
- 荣获2025中国AI技术应用产业全景图谱-行业应用层-法律事务业务支撑层-法律服务
- 参与编写《生成式人工智能知识产权运营管理指南》、《人工智能大模型私有化部署技术实施与评价指南》等一系列行业有影响力的文件

01

近期热点

近期热点

• Sora 2来了！OpenAI：迈入视频领域的“GPT-3.5时刻”

2025 年 10 月 1 日,OpenAI 正式发布了 Sora 2,这是自 2024 年原版 Sora 发布以来最重大的技术升级。OpenAI CEO Sam Altman 在发布会上表示,如果说原版 Sora 是"视频生成的 GPT-1 时刻",那么 Sora 2 就是 "视频生成的 GPT-3.5 时刻",**标志着 AI 视频生成技术从实验性阶段进入实用化阶段。**

此次发布不仅仅是模型能力的提升,更是产品形态的全面进化。Sora 2 采用了三种产品形态:核心 AI 模型、社交应用 Sora App、即将推出的 API 接口,构建起完整的视频生成生态系统。

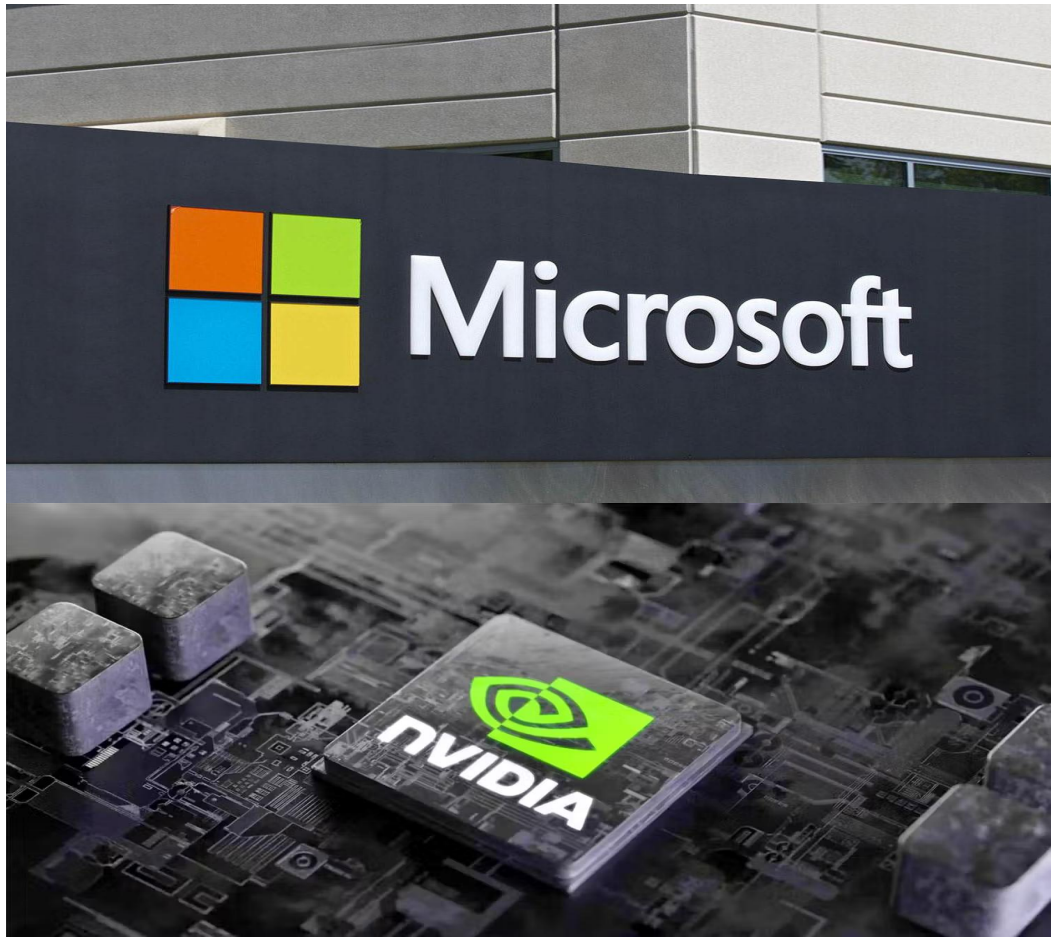
与原版 Sora 相比,Sora 2 在物理准确性、视频时长、真实度和可控性方面都有显著提升。更重要的是,Sora 2 首次实现了 音视频同步生成,并引入了革命性的 Cameo 功能,允许用户将自己或朋友带入 AI 生成的场景中。

近期热点

• 微软与Lambda达成数十亿美元的人工智能基础设施协议

财联社11月4日电，微软与人工智能云初创公司Lambda宣布达成数十亿美元AI基础设施协议。作为协议的一部分，Lambda将部署由数万块英伟达GPU支持的AI基础设施。

微软与Lambda的巨额合作表明，拥有强大算力（特别是英伟达GPU）的AI基础设施已成为科技巨头竞争的核心战场。这类大规模投入将持续推动大模型和相关应用的发展。



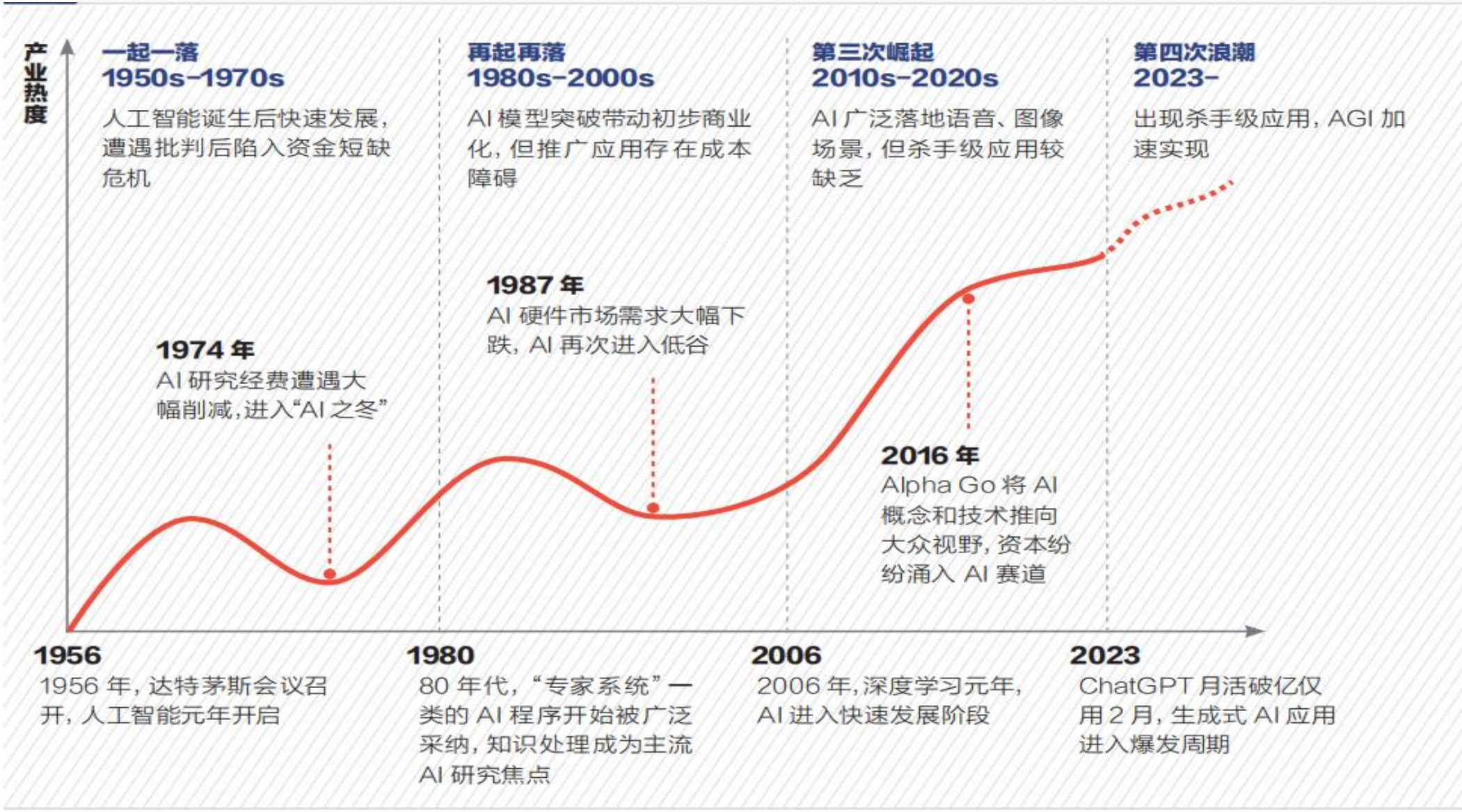
02

人工智能的发展与定位

“技术创新对生活的影响是巨大的，但这并不是自动发生的。它取决于我们发明的技术类型以及我们如何使用它们。”

——2024 年诺贝尔经济学奖获得者、麻省理工学院教授达伦·阿西莫格鲁（Daron Acemoglu）

AI 经历“三起两落”，迎来第四次浪潮



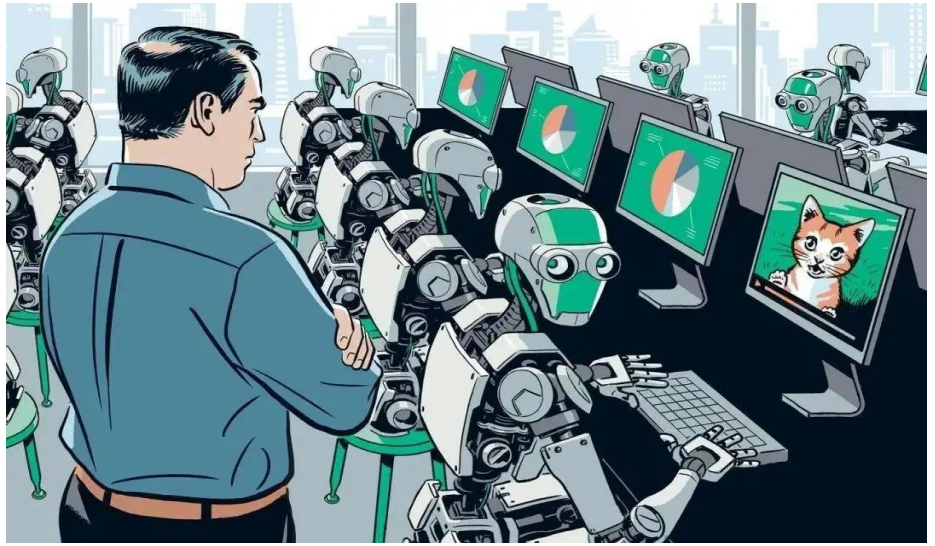
现阶段人工智能法律地位

弱人工智能时代　强人工智能时代　超人工智能时代

人工智能业界把人工智能按照先进程度分为：弱人工智能、强人工智能、超人工智能三类。按照现在人工智能的发展阶段，**人工智能还处于“弱人工智能时代”**。弱人工智能是指人类设计并创造的人类智能的某些方面，其不能完全脱离人类的控制运行。

对于弱人工智能来说，人工智能仅仅是一种行为，其本身并不能构成法律上的主体资格。人工智能是主体行为借助的工具，因此是主体的行为的一种方式，是主体行为的延伸。

人工智能是主体的法律行为。赋予它们以人格，就目前来看，显然并没有必要。



获取人工智能数据的方式

1 **自行采集** 如通过网站、App、智能家居设备等渠道收集数据

2 **第三方采购** 直接从第三方数据供应商采购

3 **技术抓取** 通过网络爬虫等技术手段抓取现有数据。前两种方式AI数据来源相对确定，主要问题在于如何获得数据所有者及涉及的其他权利人的授权。而技术抓取的数据，数量庞大且来源广泛。

03

人工智能的法律风险及监管政策

使用AI数据的法律风险

（一）侵害人格权的风险

AI数据可能包括图形、视频、音频等，而如果其中涉及自然人的形象、声音、个人信息等内容，应关注其侵害人格权的风险。《民法典》总则编第一百一十条规定，自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。第一百一十一条规定，自然人的个人信息受法律保护。AI数据可能涉及的人格权，主要包括上述权益中的肖像权、隐私权和个人信息权益。

案例tips

美图秀秀、醒图等图片编辑APP纷纷推出“AI写真”服务，用户只需上传自己的照片，等待几分钟后便可获得精美的写真艺术照，但用户无法确保自己所上传的照片仅会被运用到自己所授权的写真制作中。

使用AI数据的法律风险

（二）侵害商业秘密的风险

AI数据作为重要的商业信息，很多企业通过商业秘密的方式予以保护，若AI数据满足商业秘密的条件，以不正当手段获取权利人的商业秘密、以及使用以上述手段获取的商业秘密均属侵权行为。

一般而言，公开的数据因其不符合“不为公众所知悉”的要件，较难被认定为商业秘密，但如果企业在用户协议、隐私政策等文件中将其界定为“商业秘密”，依然可以表明此类数据的重要价值，从而可能通过《反不正当竞争法》第二条的原则性条款予以保护。

使用AI数据的法律风险

（三）构成不正当竞争的风险

除了《反不正当竞争法》具体条文中规定的侵害商业秘密行为，经营者实施其他不正当行为，还有可能被认定为违反原则性条款的不正当竞争行为。如企业通过Open API、爬虫等技术手段，取得AI数据且不加修改地使用数据，可能被认定为搭便车、构成混淆等不正当竞争行为。

案例tips

新浪微博诉脉脉获取使用“微博用户信息”案

法院虽然没有认定被告有侵害商业秘密的不正当竞争行为，但一审法院将“《开发者协议》中将用户信息定义为微博商业秘密”作为考量因素，认定了用户信息的重要价值，亦对案件定性产生了影响，同时法院也确立了**使用Open API模式获取数据应遵循“用户授权”+“平台授权”+“用户授权”的三重授权原则，否则存在较大的不正当竞争的法律风险。**

使用AI数据的法律风险

（四）侵害著作权的风险

企业使用的AI数据，可能包含文字、图像、音视频资料等内容，这些内容可能构成受我国《著作权法》的保护的作品或录音录像制品，**未经授权使用他人作品**，存在侵害著作权的法律风险。

企业在训练人工智能使用AI数据的过程中，一般会将相关AI数据复制或者下载到自己所有或者第三方服务器中进行保存以便于使用，该种行为属于著作权中的**“复制”**行为。而企业对AI数据的使用，一般系用于自身商业目的之使用，并不满足《著作权法》第二十四条所明确规定的“合理使用”的条件。在此情况下，使用他人作品，应获得权利人的明确授权，以避免产生著作权侵权法律责任。

大众点评网诉爱帮网侵害“点评信息”著作权案、湖南卫视诉内聚公司等侵害《歌手》节目信息网络传播权案.....

情节严重的，亦有构成侵犯著作权罪的刑事风险。

使用AI数据的法律风险

（五）其他刑事风险

在获取AI数据的过程中，如违反了《刑法》规定，造成严重后果的，还会面临其他刑事风险。这些风险主要来源于获取行为的非法性，其中以**破坏技术措施、非法侵入、干扰计算机系统**正常运行为主要风险来源。

案例tips

上海晟品公司及其职员采用技术手段非法抓取科技公司服务器中存储的视频数据，破解科技公司的防抓取措施，情节严重，构成**非法获取计算机信息系统数据罪**。

我国对人工智能的治理途径

1 **法律法规制定**

2024年9月24日，**《网络数据安全管理条例》正式出台**，自2025年1月1日起施行。作为网络安全法、数据安全法、个人信息保护法三法的下位配套规范，《网络数据安全管理条例》的出台**弥补了我国数据治理领域全位阶法律规范体系中“行政法规”的缺失**，为三法框架下的制度衔接与协调、规则细化与补充提供了解决方案，在网络数据安全保护领域起到纲领性作用，也为贯彻落实“坚持高质量发展和高水平安全良性互动”理念提供了重要范式。

2 **政策引导与扶持**

中共中央在**《关于进一步全面深化改革推进中国式现代化的决定》**中明确提出，要完善生成式人工智能发展和管理机制，加强网络空间法治建设，健全网络生态治理长效机制，建立人工智能安全监管制度等。工信部等四部门发布**《国家人工智能产业综合标准化体系建设指南（2024版）》**，要求完善治理标准，规范人工智能的技术研发、运营服务和全生命周期治理。

我国对人工智能的治理途径

3 **安全监管体系建设**

制定人工智能安全标准、建立安全评估体系、加强安全监测和预警等，确保人工智能技术在应用过程中始终处于可控状态。如**《生成式人工智能服务管理暂行办法》**对生成式人工智能服务的提供与使用做出规范，包括技术发展、服务规范、监督检查和法律责任等。

4 **科技伦理审查**

出台**《科技伦理审查办法（试行）》**，对包括人工智能在内的科技领域进行伦理审查，确保人工智能的研发和应用符合伦理原则，防范技术滥用等风险。

5 **国际合作与共治**

积极倡导国际合作与全球共治，发布**《全球人工智能治理倡议》《人工智能全球治理上海宣言》**，坚持“以人为本、智能向善”，为世界提供了基于人类命运共同体理念的人工智能治理新视角，为全球人工智能治理积极贡献中国智慧。

我国对人工智能的治理途径

在**数据与算法偏见**方面，我国已于2022年1月由国家网信办、工信部、公安部、国家市场监督管理总局联合发布**《互联网信息服务算法推荐管理规定》**，该规定针对算法歧视、“大数据杀熟”、诱导沉迷等进行了规范管理，并要求建立算法分级分类安全管理制度。

在**内容虚假与伪造**方面，**《互联网信息服务算法推荐管理规定》**亦要求对算法生成合成的信息做显著标识，并要求提供互联网新闻信息服务的算法推荐服务提供者和使用者，不得生成合成虚假新闻信息。**《互联网信息服务深度合成管理规定》**则更加细致地规定了包括智能对话、智能写作、人脸生成、人脸操控、姿态操控等具有生成或显著改变信息内容功能的深度合成服务应当遵守的要求，包括以显著标识的形式向公众提示。

类别	文件
政策	《新一代人工智能发展规划》 《促进新一代人工智能产业发展三年行动计划（2018-2020）》 《国家新一代人工智能开放创新平台建设工作指引》
法律	《网络安全法》 《数据安全法》 《个人信息保护法》 《科学技术进步法》
人工智能及算法相关的行业管理规定	《网络音视频信息服务管理规定》 《网络信息内容生态治理规定》 《智能网联汽车道路测试管理规范（试行）》 《人工智能医疗器械注册审查指导原则》 《人工智能辅助诊断技术管理规范》 《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
人工智能及算法专门规定及配套标准	《关于加强互联网信息服务算法综合治理的指导意见》 《互联网信息服务算法推荐管理规定》 《互联网信息服务深度合成管理规定》 《生成式人工智能服务管理暂行办法》 《信息安全技术 机器学习算法安全评估规范 GB/T 42888-2023》 《生成式人工智能服务安全基本要求（征求意见稿）》

我国对人工智能的治理途径

在**数据与隐私泄露**方面，我国**《数据安全法》**已明确将数据分类为国家核心数据、重要数据、一般数据，进行轻重有别的差异化保护。此外，在**《网络数据安全管理条例》**第9条中亦规定“在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度”。2022年12月，中共中央、国务院发布**《关于构建数据基础制度更好发挥数据要素作用的意见》**，提出建设数据产权制度、流通交易制度、收益分配制度、安全治理制度四大制度。

在**生成式人工智能**方面，我国多部委联合发布**《生成式人工智能服务管理暂行办法》**，针对生成式人工智能所面临的数据与算法偏见、内容虚假与伪造、数据与隐私泄露等困境作出了回应，这是我国为应对生成式人工智能这一新技术冲击所作的尝试。此外，《网络数据安全管理条例》等相关法规政策也对生成式人工智能作出了规定，如要求网络数据处理者采取有效措施保护数据安全，防止数据泄露和滥用等，为生成式人工智能的健康发展提供了规范和保障。

类别	文件
政策	《新一代人工智能发展规划》 《促进新一代人工智能产业发展三年行动计划（2018-2020）》 《国家新一代人工智能开放创新平台建设工作指引》
法律	《网络安全法》 《数据安全法》 《个人信息保护法》 《科学技术进步法》
人工智能及算法相关的行业管理规定	《网络音视频信息服务管理规定》 《网络信息内容生态治理规定》 《智能网联汽车道路测试管理规范（试行）》 《人工智能医疗器械注册审查指导原则》 《人工智能辅助诊断技术管理规范》 《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》
人工智能及算法专门规定及配套标准	《关于加强互联网信息服务算法综合治理的指导意见》 《互联网信息服务算法推荐管理规定》 《互联网信息服务深度合成管理规定》 《生成式人工智能服务管理暂行办法》 《信息安全技术 机器学习算法安全评估规范 GB/T 42888-2023》 《生成式人工智能服务安全基本要求（征求意见稿）》

我国对人工智能的治理途径

- 开展“清朗·网络平台算法典型问题治理”专项行动

五大问题：

- 同质化推送营造“信息茧房”
- 违规操纵干预榜单炒作热点
- 盲目追求利益侵害新就业形态劳动者权益
- 利用算法实施大数据“杀熟”
- 算法向上向善服务缺失侵害用户合法权益

三个时间点：

组织企业自查自纠
（即日起至2024年12月31日）

↓

核验企业自查情况
（2025年1月1日至2025年1月31日）

↓

深入评估治理成效
（2025年2月14日前完成）

我国对人工智能的治理途径

- **开展“清朗·网络平台算法典型问题治理”专项行动**

清单指引：

算法专项治理清单指引

序号	核验项目	核验要点	核验内容
1	信息茧房	用户兴趣选择	1.平台不得强制用户选择兴趣标签，允许用户跳过标签选择页面。
2		用户标签管理	2.平台应提供兴趣标签查看功能，向用户展示用于内容推送的个人兴趣标签。 3.平台应向用户提供用于个性化推荐服务的个人兴趣标签管理功能。 4.平台应向用户提供便捷的关闭算法推荐服务的选项。用户选择关闭后，平台应立即停止算法推荐服务且不影响用户正常使用，不得频繁通过弹窗等方式提醒用户开启。
3		“不感兴趣”功能设置	5.平台应向用户提供“不感兴趣”等功能选项，如“对话题不感兴趣”“对内容质量不满意”“此类内容过多”“重复推荐”等。用户操作后，平台应减少同类内容推送频率。
4		防沉迷举措成效	6.平台应构建用户沉迷防范机制，及时总结相关成效，配合有关部门的监督检查工作。 7.平台应具备针对“信息茧房”“同质化推荐”等网民重点关注问题的防范举措，通过内容去重、打散干预等策略提升推送内容多样性丰富性，及时总结相关成效，配合有关部门的监督检查工作。
5		个人信息权益保障	8. 平台应向用户告知用于内容推送的收集处理的个人信息种类，并征得用户同意。
6	热搜榜单	算法规则公示	9.平台应公示榜单排序机制机理，如基本原理、排序依据、主要因素等详细信息，并通过事例予以说明。
7		日志留存核验	10.平台应留存榜单相关网络日志，日志内容包括时间、榜单排名、热度值计算相关数据等信息，配合有关部门的监督检查工作。
8		水军账号识别	11.平台应健全异常账号监测机制，防范违规操纵榜单、控制热搜等现象，总结相关成效，配合有关部门的监督检查工作。
9	新就业形态劳动者权益	算法优化效果	12.平台应统计算法升级后订单超时率、平均配送超时率、交通事故发生率等相关数据，留存相关数据及日志，配合有关部门的监督检查工作。
10		规则透明度	13.平台应公示配送时间预估、路线规划、配送费用计算明细等相关算法机制机理。
11		申诉渠道	14.平台应向用户提供申诉和公众投诉、举报入口，及时处理用户反馈。 15.平台应说明申诉处理流程、反馈时间等信息，公开近期申诉成功案例，留存处理日志，配合有关部门的监督检查工作。
12	大数据“杀熟”	差异化定价	16.平台不得存在相同商品不同用户原始定价不一致情况。
13		优惠规则公示	17.平台应说明优惠促销规则，如适用范围、参与条件、特定限制等。 18.对于使用优惠券的场景，平台应说明优惠券发放范围、用户身份限制、发放数量、使用条件等信息。 19.在订单结算页面，平台应展示优惠券、满减规则等优惠明细。
14		优惠券领取失败原因	20.平台应向用户说明优惠券领取失败的真实原因，如领取截止时间、领取要求等。
15	算法向上向善	未成年人保护	21.平台应及时总结防范未成年人网络沉迷、过度消费所采取的优化算法推荐服务措施及成效，配合有关部门的监督检查工作。
16		老年人保护	22.平台应持续优化完善面向老年人的算法推荐服务，便利老年人获取有益身心健康的信息。
17		优化内容生态	23.鼓励平台坚持主流价值导向，利用算法提升优质内容推送、识别违法网络谣言等信息。
18		生成合成信息标识	24.平台应对由自身提供算法的生成合成信息作出显著标识，及时总结检测识别生成合成信息、发现处理违法违规生成合成信息的措施及成效，配合有关部门的监督检查工作。
19	落实算法安全主体责任	算法机制机理审核	25.平台应及时总结建立算法机制机理审核的管理制度和技术措施的机制及成效，配合有关部门的监督检查工作。
20		算法模型安全评估	26.平台应定期对算法模型开展安全评估，及时总结评估成效，配合有关部门的监督检查工作。
21		数据安全	27.平台应及时总结建立数据安全管理制度和技术措施的机制及成效，配合有关部门的监督检查工作。

04

人工智能数据的合规建议

AI企业应当增强风控意识，做好数据合规工作：

（一）获得AI数据权利主体的授权

无论是肖像权、著作权还是个人信息、商业数据，**获得数据权利主体的授权**，都是合规使用数据的理想方案。

获取授权，**首先需要判断数据权益的性质与权利主体**，如果相关数据来自于第三方，还应确定原始权利主体以及授权链条的完整性。实践中，AI学习需要的数据是海量的，获得每一个数据主体的授权一般难以实现。

但对于某些风险较大的数据，如个人生物识别信息、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、病历信息等个人敏感信息（已匿名化的信息除外），应以授权同意为原则。如果是研发所必需，取得数据主体授权是研发主体难以豁免的法律义务。**在获取、使用这类数据时，应对数据的原始权利主体、授权链条、授权范围等内容进行严格的审查**。

（二）通过第三方采购数据

如（一）所述，AI研发需要的数据是海量的，逐一获取所有权利主体的授权并不现实，**从数据供应商采购数据便成为了很多企业的解决方案**。我们认为，在采购过程中，应通过协议等方式要求供应商对AI数据的知识产权，涉及第三方的民事权益（包括但不限于自然人肖像权、隐私权、个人信息）做无瑕疵或者不侵权保证，并要求该供应商确保授权权利的完整合法。如果相关数据可能涉及个人信息（尤其是个人敏感信息），应当在传输前由该第三方进行脱敏处理且做到无法还原。**通过上述约定，AI企业可以降低潜在的侵权风险，并且可以将其用作合法来源抗辩的理由。**

合规tips

建议**在协议中应明确保密义务条款**，即对企业购买的AI数据，要求供应商承担保密义务，以降低信息被披露的可能性，从而进一步降低法律风险。同时，AI企业可通过抽查的方式对供应商提供的数据权属文件进行审查，并**对相关审查情况进行书面记录**，作为潜在侵权纠纷中抗辩理由的证据，以进一步降低因购买数据而导致的潜在侵权法律风险。

（三）使用无需授权的公有领域数据

“公有领域”是知识产权法中的概念，是指在现代知识产权法体系下，不适合于知识产权保护的思想和作品的总体，是人类的一部分作品、知识的总汇，可以包括文章、艺术品、音乐、科学理论、发明等。对于已经匿名化的个人信息、政府公开数据等数据信息，亦可以将其视为广义的“公有领域”范围。

1.合理处理已经合法公开的个人信息

根据《民法典》第一千零三十六条的规定，合理处理该自然人自行公开的或者其他已经合法公开的信息，不承担民事责任，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外。国家标准《信息安全技术个人信息安全规范》3.13条亦指明，个人信息经匿名化处理后所得的信息不属于个人信息。因此合理收集与使用已经合法公开的个人信息，收集和使用经匿名化处理后的个人信息，可以最大限度地降低使用AI数据的个人信息合规风险，

2.使用公有领域的素材

根据我国《著作权法》第五条的规定，法律、法规，国家机关的决议、决定、命令和其他具有立法、行政、司法性质的文件，及其官方正式译文；时事新闻；历法、通用数表、通用表格和公式均不受著作权法保护。上述素材，可以不考虑其著作权而无偿使用。此外，《著作权法》亦规定了作品的复制权等著作财产权具有一定的保护期限。对于已经超过著作权法保护期限的作品，任何主体都可以就该作品无偿使用。

（四）合规使用爬虫等技术手段

企业通过爬虫、Open API等技术手段获取AI数据，应保证目的正当、手段合法。从防范风险的角度，建议**企业建立配套的数据安全系统及专门的合规审查机制**，重点关注爬虫行为的合规性（遵守robots协议、遵循“三重授权原则”等），爬取数据内容的合规性（甄别所爬取数据内容、获取权利人授权）以及对所爬取数据进行使用、储存的合规性。

（五）限定AI数据的使用范围，建立安全机制

在AI数据使用过程中，**建议企业对数据的使用、披露范围进行严格控制**。通常情况下，企业的AI数据仅用于人工智能研发，因此**建议企业通过内部规章制度或者员工保密协议**，将数据的适用范围限制在“内部使用”。除了人工智能训练之外，如没有特别需求，建议企业不再将AI数据转授权或者对外公开、许可或转让，以降低可能的侵权风险。作为掌握大量AI数据的主体，**建议企业建立数据安全系统，设定合规审查机制**，这样一方面可以保护公司数据财产安全，另一方面也是企业法定的数据合规义务。

（六）加强内部员工培训考核

训练人工智能数据的合规使用是企业数据合规中的一部分，面对新工具、新场景，企业对相关部门的员工做针对性培训。**多样化的培训方式加上必要的考核机制**，可以帮助员工尊重和理解训练数据使用的合规要点，有助于员工在具体的工作中落地企业要求。

（七）畅通投诉，举报渠道，优化技术措施

《生成式人工智能服务管理暂行办法》第15条规定“提供者应当建立健全投诉、举报机制，设置便捷的投诉、举报入口，公布处理流程和反馈时限，及时受理、处理公众投诉举报并反馈处理结果。”**建议企业应当建立健全投诉、举报机制**，方便权利人通过便捷的途径保护自身合法权利。对于投诉、举报人工智能生产内容涉嫌侵犯在先作品权利的情形，企业应及时处理，**通过数字水印技术实现人工智能合成内容的追踪溯源**，防止知识产权剽窃。

福建新世通律师事务所
FUJIAN NEW STONE LAW FIRM

以法赋能数字经济与人工智能

福建新世通律师事务所