汉坤法律评述

2021 年 4 月 27 日

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

欧盟发布人工智能新规草案

作者：段志超 | 蔡克蒙 | 王雨婷 | 胡敏喆[1]

一、要点归纳

- 欧盟委员会发布的人工智能法律框架草案提出了基于风险的规制措施。根据使用目的及所含风险的不同，草案将人工智能系统分为完全不可接受风险、高风险、有限的风险和低风险等不同等级。
- 草案禁止部署存在不可接受风险的系统，对高风险系统的部署和应用提出了一系列强制义务，包括建立风险管理系统，确保数据质量、记录并提供技术信息、留存系统日志、向用户充分告知、采取人工干预措施、确保网络安全等。
- 新规对高风险系统供应商提出了包括开展合格性评估（conformity assessment）等一系列法律要求，要求进口商确保外国供应商完成相应的评估并在相关系统上附带认证标识。
- 出海人工智能企业应当梳理欧盟监管机构提出的各项要求，逐项完善并编制相关资料，应采购方要求提供相关文件，配合完成可能适用的合格性评估。

二、背景

4 月 21 日，欧盟委员会提出新的人工智能法律草案，将作为欧盟统一的人工智能规则（人工智能法）并修正某些联盟现有立法（Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts，**“草案”**）[2]，为人工智能系统风险评估，部署和应用提供依据。

三、草案的适用范围

根据草案序言第 2 条，在欧盟内部或第三国设立的在欧盟市场投放或使用人工智能系统的供应商、位于欧盟内的人工智能系统使用者、由欧盟境外主体提供但被部署于欧盟境内或者对欧盟境内个人产生影响的人工智能系统的供应商和使用方均需要遵守草案的有关规定。

值得注意的是，根据草案第 25 条，在无法识别进口商的情况下，欧盟以外的供应商应在其系统投放到

[1] 实习生吴东璇对本文的写作亦有贡献。

[2] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.

欧盟市场之前通过书面授权在欧盟内指定一名授权代表。授权代表应保留一份欧盟合格性声明和技术文件的副本，并在合理要求下向国家主管机关提供所有必要的信息和文件。

四、草案对人工智能系统的风险分级

草案提出了基于风险的规制措施。草案首先划定了四个风险级别，包括不可接受的风险（Unacceptable risk）、高风险（High-risk）、有限的风险（Limited risk）和最小风险（Minimal risk）。具体而言：

不可接受的风险是指人工智能系统的部署和应用违反基本人权。草案第 5 条规定了四类不可接受的风险：

- 在无意识中对人类意识进行操控，从而影响其决定或扭曲其行为，进而对人类造成身体或心理的伤害；
- 利用特定人群因年龄、身体或精神残疾而存在的任何脆弱性，实质性地扭曲与该人群有关的行为，以导致或可能导致其身体或心理受伤害；
- 公共机构或其代表用以根据自然人的社会行为、已知或预测的个性特征，在一定时期内对自然人的信誉进行评估或分类，导致对某些自然人或整个群体的有害或不利待遇；
- 除极个别例外场景（如搜寻被害人、防止明确实质且紧迫的危害以及追查犯罪嫌疑人），**在公共场所基于执法目的使用实时远程生物识别系统**[3]。

高风险是指人工智能系统的部署和应用会对个人的安全或基本权利[4]造成不利的影响。这些高风险的人工智能系统需要在符合某些强制性要求和事前合格性评估的情况下，才能进入欧洲市场。草案的附件三列举了高风险系统，包括：

- 生物识别领域：如“实时”和“事后”远程生物识别的人工智能系统；
- 关键基础设施领域：如道路交通管理以及水、气、热和电力供应的安全组件；
- 教育和职业培训领域：如招生录取及考试评定；
- 就业领域：如简历评估、工作任务分配与工作表现评估；
- 私人服务与公共福利领域：如资信评估、公共福利分配；
- 执法领域：如用于测谎仪、情绪状态监测、证据可靠性评估、犯罪风险评估的人工智能系统；
- 移民与边境管理领域：如核实旅行证件的真实性、评估移民风险；

[3] 根据草案的定义，“远程生物特征识别系统”是指一种 AI 系统，其目的是通过将人的生物特征数据与参考数据库中包含的生物特征数据进行比较来在远处识别自然人，并且人工智能系统使用者事先不知道该人是否会在场并能够被识别；“‘实时’远程生物特征识别系统”是指一种远程生物特征识别系统，在此过程中，生物特征数据的捕获，比较和识别均没有明显的延迟（包括即时识别和有限的短暂延迟）。

[4] 如获得社会保护、自由行动、不受歧视、保护私人生活和个人数据、人格尊严等权利。

- 司法领域：如帮助司法部门研究和解释事实和法律，将法律适用于具体的案件。

五、高风险系统部署和应用要求

草案并未绝对禁止高风险系统的部署和应用。为了促进欧盟委员会和成员国在人工智能领域的工作，并提高对公众的透明度，所有高风险人工智能系统的供应商应在独立运行的高风险人工智能系统投入市场前进行合格性评估，并在欧盟委员会建立和管理数据库中进行登记。草案在第二章（第 9-15 条）中对高风险系统开发、部署和应用提出了一系列要求。具体包括：

- 建立、部署、记录和维持贯穿高风险系统始终的适当的风险管理系统（第 9 条）；
- 使用高质量的训练、确认和验证数据集，数据集应相关、具有代表性、无误且完整，以最大程度地降低风险和歧视性结果（第 10 条）；
- 编制监管部门要求提供的技术信息（具体应包含草案附件四中的全部内容），以便监管部门评估系统的合规性（第 11 条）；
- 设计和开发高风险系统应使其具备自动记录系统的日志记录功能，以确保系统运行状态全生命周期的可追溯性（第 12 条）；
- 向人工智能系统使用者提供清晰、充分的信息（第 13 条）；
- 采取适当的人工干预措施，以最大程度地降低风险（第 14 条）；
- 确保准确性、稳健性和网络安全（第 15 条）。

六、高风险系统供应商合规义务

草案第三章对高风险系统供应商提出了一系列法律要求，包括：

- 确保高风险系统符合第二章规定的全部强制义务；
- 建立、部署适当的质量管理系统；
- 根据草案附件四的要求编制技术信息文件；
- 在系统运营前或者系统功能有实质修改时开展合格性评估；
- 自动生成日志记录并根据具体的应用场景和法律规定保存一定的时间；
- 如果发现存在不合规的情形，应当采取相应的补救措施；
- 如果发现系统存在风险，应当及时告知监管机构不合规的事项和采取的措施；
- 供应商应建立并记录上市后监测系统，其方式应与人工智能技术的性质和高风险人工智能系统的风险相适应；

- 高风险人工智能系统出现任何系统故障或严重事故时，供应商有义务立即向主管部门报告，最迟不超过故障或事故发生后 15 天，以使有关部门能对其实现有效监管；

- 市场监管机构有权访问供应商使用的培训、验证和测试数据集的权限，包括通过应用程序编程接口（API）或支持远程访问的其他技术手段。

七、草案对高风险系统使用者合规义务

草案第 29 条要求高风险系统使用者按照系统附带的使用说明使用此类系统，且在系统出现或可能出现故障或事故时，使用者有义务及时通知供应商并暂停使用系统。另外，高风险人工智能系统的使用者在适当期限内应保留系统自动生成的日志，并将日志作为有关内部治理安排、流程和机制的文件的一部分进行维护。

八、特定人工智能系统的透明度规则

草案第四部分对旨在与自然人互动的人工智能系统、情感识别系统和生物特征分类系统以及用于生成或操纵图像、音频或视频内容的人工智能系统提出了透明度规则。使人工智能系统使用者可以在知情的情况下决定是否继续使用人工智能系统。对于高风险系统，第三部分提出了更为严格的透明度规则（见前述“3. 草案对高风险系统的部署和应用提出的强制义务”），而符合前述条件的中低风险系统则仅需履行一般性的告知义务。

九、处罚规则

草案第 71 条规定了两档处罚金额，如果企业未遵守第 5 条有关禁止人工智能的要求或者第 10 条有关数据质量的要求，最高将面临 3,000 万欧元的处罚或者企业上一年度全球营业额 6%的处罚，以较高者为准。除此之外，如果企业违反其他要求，最高将面临 2,000 万欧元的处罚或者企业上一年度全球营业额 4%的处罚，以较高者为准。

十、草案的影响

草案是全球主要法域首部关于人工智能应用的系统、全面的法律提案，体现欧盟一直以来对个人自主、人格尊严、反歧视等基本人权的重视。草案采取风险规制的思路，根据对基本人权的风险将人工智能系统划分为不同等级进行监管，体现了欧盟引领人工智能立法，为全球人工智能立法树立标杆的雄心，无疑将对全球其他国家和地区的人工智能立法起到示范作用。

草案的正式出台虽仍需时日，但对有出海计划的国内人工智能企业仍可起到风向标的作用。企业应避免在欧洲开展被草案认定为不可接受风险领域的业务，并谨慎开展高风险领域的业务，考虑对拟投入欧盟市场的高风险人工智能系统，在设计开发阶段即植入透明度、可溯源、人工干预等措施，确保数据质量、防止数据歧视，加强产品运行的记录与监控。特别值得注意的是，在公共场所基于执法目的使用实时远程生物识别系统在绝大多数情况下均被视为存在不可接受的风险，这意味着相关业务在欧盟市场很可能前途暗淡。而用于自然人的“实时”和“事后”远程生物识别的人工智能系统，包括此类商用系统，被视为具有高风险，这意味着企业需要在设计开发阶段落实草案提出的高风险合规措施，将合规考量纳入产品设计、开发的早期阶段。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com