



宁人律师事务所
NING REN LAW FIRM

大模型企业出海 法律实务报告

Legal Practice Report for Large
Model Enterprises Overseas Expanding

牵头单位：宁人律师事务所、北京中关村高新技术企业协会
集智未来、北京智谱华章科技有限公司



宁人研究院

更多免费行业报告

并购家

www.ipoiipo.cn

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费



宁人律师事务所
NING REN LAW FIRM

大模型企业出海 法律实务报告

Legal Practice Report for Large
Model Enterprises Overseas Expanding

宁人研究院

编 写 组(按拼音首字母排序)

陈 骋 陈晓芳 甘青锋 郭苏敏 呼娜英 姜 赫
姜 倩 李嘉英 李 菡 李迪娜 刘建国 刘 薇
刘 媛 马 军 马星烁 马阳明 买尔旦 石 霖
史 馨 司乃捷 王海棠 温 馨 吴佳丽 吴少卿
张 晨 张 戈 张小虎 买热叶木 努尔麦麦提

参 与 单 位

北京智谱华章科技有限公司
三六零安全科技股份有限公司
北京零一万物科技有限公司
深圳市华为数智信息技术有限公司
北京中科闻歌科技股份有限公司
北京深度求索人工智能基础技术研究有限公司
北京合思信息技术有限公司
北京微步在线科技有限公司
北京光年无限科技有限公司
重庆艾瑞数智科技有限公司



第一章 主体设立与架构设计

第一篇 境外主体设立中的考量	002
一、境外主体是否需要设立的影响因素	002
二、选择理想的东道国：策略与考量	003
三、设立主体的类型	004
四、境内外主体间隔离	005
五、过渡阶段的安排	006
第二篇 以协议控制模式设立境外主体	007
一、协议控制模式的基本路径	007
二、以协议控制模式设立境外主体的优势与不足	008
三、协议控制模式对企业在中国上市的影响	009
第三篇 以信托模式设立境外主体	011
一、以信托模式设立境外主体的优势与不足	011
二、以信托模式设立境外主体的基本路径	012
三、以信托模式设立境外主体的风险及应对	014
第四篇 主体设立中的税务因素	016
一、出海企业税务筹划的重点关注	016
二、特定国家/地区的税收管理规定	018

第二章 境外投资审批及境外融资架构

第一篇 中国企业境外投资的审批与监管	026
一、商务主管部门备案(或核准)	026
二、发改委备案(或核准)	026
三、外汇登记	027
第二篇 搭建公司架构的类型与选择	028
一、公司架构的常见类型	028
二、选择公司架构的考量因素	029
第三篇 搭建红筹架构的惯常操作步骤	030
一、大红筹和小红筹	030
二、搭建红筹架构的惯常步骤	031

第三章 跨境劳动法遵从

第一篇 企业跨境用工安排：模式、法律风险及应对

.....034

一、跨境用工安排的现有模式 034

二、跨境用工安排涉及的法律风险 035

三、跨境用工的合规建议 041

第二篇 涉外劳动关系的识别及法律适用 049

一、涉外劳动关系的识别 049

二、涉外劳动纠纷中法律适用的常见情形及利弊分析 052

三、如何在涉外劳动争议中适用中国劳动法律法规 056

第四章 人工智能产品法规遵从

第一篇 全球人工智能法规概览 058

一、欧盟《人工智能法案》及成员国法规 058

二、美国人工智能相关标准、规则与法案 060

三、其他主要国家与地区性法规 062

第二篇 人工智能产品出海合规要点分析 066

一、大模型训练与开发阶段的合规要求及企业应对 066

二、人工智能产品运营方式的合规要求及企业应对 070

三、人工智能产品部署阶段的合规要求及企业应对 073

第三篇 人工智能产品出海的文化适应与未成年人保护

.....077

一、全球化背景下的人工智能产品的文化适应 077

二、企业应对文化与价值观差异的合规策略 081

三、人工智能产品未成年人保护合规要点 083

第四篇 人工智能产品出海之特殊行业合规要点 085

一、医疗行业中人工智能产品的合规要点 085

二、金融行业中人工智能产品的合规要点 088

三、制造业中人工智能产品的合规要点 091



第五章 数据合规

第一篇 企业境外经营过程中的数据合规要点	094
一、目标市场适用数据法规的识别	094
二、公司内部数据合规体系的构建	095
三、用户信息处理的原则与规范	097
第二篇 大模型企业数据出境合规	100
一、大模型企业主要数据出境场景	100
二、我国对数据出境的法律监管	101
三、数据出境合规建议	106
第三篇 目标市场数据出境规则的遵循	107
一、数据本地化存储	107
二、数据出境	108
三、企业应对目标市场数据出境监管的合规措施	111

第六章 知识产权全球布局与保护

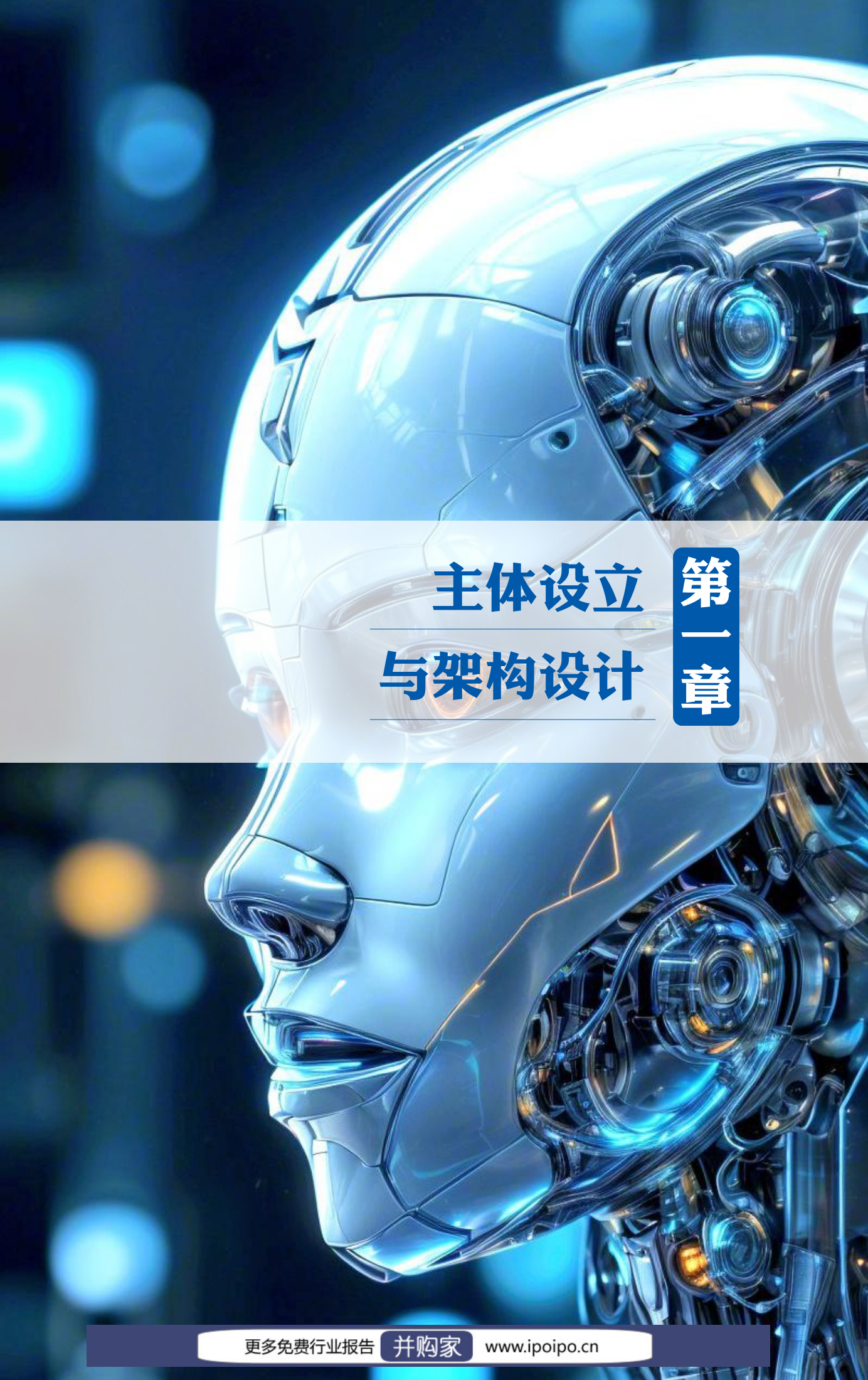
第一篇 全球知识产权策略与布局	114
一、大模型企业全球知识产权布局策略	114
二、国际知识产权法律体系	115
第二篇 人工智能企业出海知识产权保护体系建设 与侵权案件诉讼策略	121
一、人工智能企业出海知识产权保护体系建设	121
二、侵权监测要点	123
三、跨国知识产权诉讼策略	123
第三篇 大模型企业核心知识产权保护 路径分析与建议	125
一、大模型企业核心知识产权保护路径概述	125
二、闭源大模型的知识产权布局与权利保护	127
三、模型开源策略分析与建议	130
四、大模型企业核心知识产权保护策略的建议	132

第七章 全球化法律支持与协作

序言	134
一、全球化法律支持部门的构建与管理	134
二、全球化法律支持部门的运作模式	136
三、法律支持部门面临的全球化管理挑战	139
四、外部法律服务机构的选择与有效利用	142
结语	144

第八章 出口管制与合规

第一篇 人工智能技术出口管制与应对策略	146
一、我国对外贸易管制概述	146
二、人工智能技术出口的分类规制	147
三、企业人工智能技术出口合规路径	149
第二篇 美国人工智能算力管制对人工智能 企业出海的影响及风险规避	150
一、美国人工智能算力管制政策	150
二、美国人工智能算力管制标准	153
三、人工智能企业应对美国算力出口管制的合规建议	156
第三篇 美国大模型管制对我国人工智能出海 影响剖析与应对措施	158
一、美国大模型管制政策概述	158
二、我国人工智能出海受美国大模型管制的可能影响	160
三、我国人工智能企业的应对措施	162



主体设立 与架构设计

第一章

第一篇 境外主体设立中的考量

一、境外主体是否需要设立的影响因素

大模型企业在制定出海战略时,一个重要的决策事项是境外主体的设立与否。本章将介绍一些大模型企业在决定是否设立境外主体时必须考量的因素,为大模型企业的境外主体设立活动提供参考。

(一)业务范围与模式:决定性因素

大模型企业出海必须首先确定业务模式和业务场景,这有利于设立境外主体以及此后一系列决策。如企业仅计划向海外B端客户销售标准化的大模型本地授权,则直接与境外主体订立合同即可,并不需要在境外设立主体。但若企业计划在境外开发ToC应用,则可能因数据跨境合规等要求,需要在境外设立主体。

(二)合规强制性要求

企业在决定是否设立境外主体时,需要谨慎考虑目标市场的合规性要求。例如,沙特阿拉伯要求,若要在当地开展商务活动,必须在当地设立商事主体。再如,欧盟对于个人数据的跨境传输,尤其是外国主体处理欧盟个人数据有着非常严格的要求,处理欧盟个人数据的企业,若不在欧盟设立主体,则将面临非常高昂的合规成本(具体要求详见本报告数据合规相关章节)。此外,企业还可能因目标市场在外汇、财税、外贸甚至环保等各方面的合规要求而必须设立海外机构。

(三)劳动用工需求

大模型企业是否在境外设立主体也与其境外的劳动用工需求有关。例如,从事B端业务的企业因其业务模式可能需要本地化的销售、实施和售后团队;开展ToC业务的企业则可能需要本地的合规、运营、客服等人员。为解决境外员工的薪酬发放、社会保险缴纳等合规和成本问题,企业可能需要在用工地设立境外主体。

(四)文化与价值观融入

大模型往往涉及内容的生成,在中文语境下训练的模型极有可能与目标市场的文化并不兼容,甚至出现触犯文化禁忌的内容。例如,伊斯兰教、犹太教都禁食猪肉,印度教徒不吃牛肉,在特定文化场景下出现食用某种食物的描写可能冒犯相应的用户。不同的海外市场对同一问题的认知也有所不同,当前英美主流价值观高度推崇LGBT+同权,任何反对此倾向的言

论都会受到舆论抵制,但在伊斯兰国家同性恋行为则会触犯刑法,对该种行为的描述也可能冒犯当地主流价值观。因此,大模型企业面对目标市场的文化和价值观差异,可能无法做到“一招鲜,吃遍天”,而是需要深入了解当地文化,并为其提供差异化服务。

(五)资金往来的便利性

我国目前对外汇仍然采取较为严格的管制措施,印度、泰国、阿根廷等发展中国家关于外汇的管理政策也较为严格。大模型企业若不在境外设立主体,则需以境内主体的名义与境外供应商、企业、用户等主体进行交易和资金往来,单笔大额交易的影响尚不十分明显,但若频繁开展境内外收支活动则可能面临一定的障碍以及合规风险。

(六)融资与上市需求

大模型企业设立境外主体的决策还与企业的融资和上市需求有关。一方面,大模型企业出海已经成为一种浪潮,成功设立境外主体,可能会引起资本的青睐,这对企业融资是一种利好因素。另一方面,存在融资和上市需求的企业,在出海时需特别注意合规性,以应对未来可能面临的关于出海过程合规性的审查。计划在香港等境外资本市场上市的公司可以将业务出海和海外上市两个目的相结合,更好地设计境外架构,在节约成本的同时更好地满足境外资本市场的财务、信息披露等合规要求。

(七)运营成本

境外主体的运营成本也需要纳入是否设立境外主体的考量之中。在境外设立和维持主体可能产生许可证费用、代办设立佣金、营业场所租金、员工用工成本、财务和法律咨询等费用,具体项目和金额在国与国间差别非常大。若没有必须设立境外主体的理由且成本过高,则企业也可以考虑暂缓设立境外主体。

二、选择理想的东道国：策略与考量

若企业决定设立境外主体,则需认真考虑设立的地点,一般而言,企业选择东道国时,如果目标市场是单一国家则一般应将境外主体设置在目标国;如果海外业务是区域性甚至全球化的,则可以参考以下要素,选择海外业务的总部。

(一)开放程度与营商环境

理想的东道国应当对外资持开放态度,不对外资设置过多的障碍。最为理想的准入政策是内外资一致,对外资不设置额外的程序和门槛,典型代表是哈萨克斯坦、乌兹别克斯坦;部分国家除特殊行业外,仅要求外资进行程序性的备案,而不进行实质性的审核,例如澳大利亚;还有一些国家要求外国投资者获取许可证后才可投资,并会对外国投资者的投资事项进行实质性审查,例如沙特阿拉伯、俄罗斯等。外资准入门槛不但会影响境外主体设立的时间和成本,更体现了一个国家对于外资的友好和欢迎程度,并持续体现在后续的外资管理中。

(二) 外资优惠政策

在设立境外主体时,也应具体分析备选国家对于外资的优惠政策。优惠政策既可以是直接的经济利益,如税收减免、运营补贴等,也可以是对商业活动的帮助,如便利的融资贷款、低价的商业用地、协助对接的商业机会等。企业还应注意,由于外资优惠政策的公布与落实可能存在差异,在进行信息收集时应尽量联系当地企业或了解当地情况的人员,以免优惠政策无法落实造成损失。

(三) 政治和经济稳定性

当今世界局势愈发波折云诡,大国间经贸摩擦不断,地区冲突甚至战争频发,一些国家和地区甚至发生政变,给企业的境外投资活动带来很大的不确定性。企业在选择东道国时,应着重考虑东道国的政治和经济稳定性。具体而言,在政治方面,既要关注目标国国内的政治稳定程度,也要注意目标国周边是否存在敌对国家和极端势力,还要关注目标国与中国之间是否存在摩擦;在经济方面,要综合考察目标国的市场大小、货币政策、汇率稳定程度、通货膨胀率等,防止金融危机波及海外资产的安全。

(四) 营商环境

营商环境的定义可以很广泛,甚至本章节的全部内容都可以称为营商环境。此处的营商环境主要指国家的法治程度、行政效率、廉洁程度等与政府相关的内容。较差的营商环境不但会影响企业的日常运营,而且会给企业产生大量额外的成本;司法的低效和不公正则可能给企业带来无法挽回的巨大损失,甚至使风险传导回国内。

(五) 基础设施完备度

大模型企业业务模式不同,对于基础设施的要求也存在差异。例如,若要开展ToC/公有云或私有云业务则需当地具有满足云计算和数据传输的电力和网络建设,如果仅出售本地化授权,则计算主要发生在客户内部,交付成本和难度也较低,基础设施的重要性也就相对降低。

(六) 合规要求与成本

出海的大模型企业作为外国投资者,也需遵守东道国的税务、个人信息保护、网络安全和人工智能等方面的合规要求。若相应合规要求过于繁杂,或对于企业要求过高,则可能导致企业合规成本过高而丧失竞争优势,甚至无法达到合规要求而产生监管风险。

三、设立主体的类型

企业在境外设立的主体类型要根据东道国的相关法律确定,但一般而言,东道国都支持以下几种设立形式。企业可以根据实际的业务需求,确定具体的设立模式。

(一)办事处/代表处

办事处和代表处适用于仅需维持商业存在,开展小规模的市场拓展等活动的企业。办事处/代表处的优势在于设立十分简单,在大多数国家仅需简单的注册/登记即可完成设立,维护的成本也十分低廉。但是与简单的程序和低成本相对应,新加坡、越南、卡塔尔等国家只允许代表处从事市场推广、商务联络等非盈利性质的活动,不允许直接订立商务合同。

(二)分支机构

企业也可以设立境外的分支机构。分支机构是办事处/代表处与法人公司之间的一种中间选择,能够订立商业合同,但又没有独立的法人地位,无法以自己的财产独立承担责任。一旦海外业务未能成功开展,分支机构的债务风险将直接传导至其总公司,因此如果企业能够选择设立独立的法人公司,又没有公司治理等特殊考量,原则上不建议以分支机构直接开展业务。

(三)法人公司

法人公司是最为常见的海外主体类型,具有独立的法人地位,能够以自己的名义开展商业活动,进行资金往来。根据东道国的不同法律,法人公司具体又可细分为有限责任公司、股份有限公司等类型,具体的要求和优劣势也不尽相同,在决策时应根据当地法律作出个案分析。

(四)非直接控股公司

考虑到风险隔离、防范制裁等因素,企业也可以通过协议控制、信托等方式设立非直接控股的公司,并在东道国开展业务。具体的考量及路径将在下文及此后文章展开。

四、境内外主体间隔离

大模型企业在设计境外架构时,应有意识地考虑在境内外主体间设立合理隔离,以防范制裁、出口管制和数据合规等风险。

首先,大模型行业本质上属于软件行业,除算力设备外其供应链对境外供应商没有绝对依赖,可以实现完全的国产化,国内大模型行业的客户也主要以国内机构和企业为主。在算力设备本身已被禁运的背景下,即使大模型企业受到制裁,其国内业务仍然有较强的抗制裁能力。相比之下,大模型企业的境外业务对于制裁风险则更加敏感,无论是供应商还是客户都可能受到外国制裁措施的影响而中断与大模型企业的业务联系。因此,在海外主体与境内主体间建立“防火墙”,有利于阻断中国企业海外业务因受到外国制裁而带来的影响。

其次,大模型企业出海的另一个重要动力是利用境外更加便捷易得的算力,在境外购置算力设备或采购云服务,依据美国出口管制规则,大模型企业的境外主体不会被认定为“中国”企业。

再次,大模型企业若运营 ToC 业务,需获取大量个人信息。美国关于禁止或限制中国企业取得美国个人信息的行政令已公开征求意见,其传统盟友也可能出台相同或类似政策。为避免未来业务受到影响,企业需要未雨绸缪,防止被监管机关识别到其境外主体与中国的联系。

最后,TikTok 在美国和印度的遭遇也告诉我们,全球冲突加剧和保护主义盛行会给出海的中国企业带来难以预料的风险。在敌对国家开展业务时避免展露自己的中国身份,可能是对企业更为安全的选择。

当然,境内外的主体隔离措施也会导致企业的境外资产在融资和上市时被认定为“权属不清晰”。如果为达到最好的隔离效果,完全隐藏境外主体与境内主体间的联系,则有可能违反上市公司的信息披露要求,也无法为海外业务带来融资吸引力。因此,大模型企业仍需在商业、融资和合规等不同目的间进行权衡,确定自己在隔离安排中的考量。境内外主体间如何实现隔离,将在此后两篇文章中进行介绍。

五、过渡阶段的安排

无论采取何种方案,境内外主体间的隔离都无法一蹴而就,其实施需要一定的时间。大模型企业为避免在实施隔离的过程中错失业务机会,可能需要在境外架构落实的同时开展业务。过渡阶段企业面临的最主要风险是暴露境内外主体间的联系,这既可能是由于自主进行市场推广和商标使用,也可能是股权转让等会留下记录的商务活动,因此企业应注意尽可能不要以境内主体或其直接控股的境外子公司的名义直接开展海外业务,若不欲披露境内外联系则不要使用境内商标商号,并在过渡阶段结束后采取资产交易而不是股权交易的方式移交海外业务。

第二篇 以协议控制模式设立境外主体

如前所述,大模型企业设计出海架构时应充分考虑在境内外主体间设置隔离。许多企业在需要隔离时,第一选择为协议控制模式,即境内主体通过协议而非股权控制境外主体,并享有相应的权益。本篇文章将介绍该种模式的路径、优劣势、潜在的风险及对于上市的影响。

一、协议控制模式的基本路径

(一)寻找合适的受托人

协议控制模式运行的基础是找到合适的受托人。合适的受托人应符合以下条件:

第一,不能是中华人民共和国大陆、香港、澳门地区公民,但可以是我国台湾地区公民。该受托人未来将作为名义股东负责设立境外主体,因此为避免境外主体被认定为中国公司,该受托人的国籍不可为中华人民共和国。

第二,必须可信可靠,为人正直。由于受托人作为名义股东享有很大权力,一旦违反约定将给企业造成极其严重的损失,因此企业必须委托可靠的受托人。最理想的选择是企业实控人持有境外国籍的近亲属,如无法实现则应考虑实控人可靠的海外关系。在缺乏海外资源的情形下,部分代办企业也可提供受托人资源,但此时不但需要细致考察受托人,还应尽可能要求代办企业为受托人的行为提供担保。

第三,最好财务情况良好,身体健康,家庭和睦。受托人如发生被强制执行、去世、离婚等会导致财产所有权变动的情形,也将对企业的境外资产安全造成很大威胁。虽然以上突发风险难以预防,但在备选受托人较多时,则可以从这些方面考察,尽量降低风险发生的概率。

(二)签订控制协议

受托人确定后,大模型企业即可安排与受托人签订控制协议。控制协议的名称、形式可以是多样化的,以符合当地法律规定为原则,既可以签订股权代持协议并在其中明确各类事项,也可以参考VIE架构签订一整套协议文件。控制协议至少应包含以下内容:

1.财产权益的归属

控制协议应明确境外主体包括股权、分红权等在内的财产权益归企业所有,或根据当地法律的要求在形式上由受托人所有,但企业有权随时要求以极低价格转让。该条款还应要求受托人将境外公司的财产与其自身的财产相分离,防止出现混同的情况。

2.出资款的承担

控制协议应明确,出资款由企业向受托人支付,由受托人向境外主体完成出资。受托人仅可将出资款用于境外主体的出资事宜,不得挪作他用。如出于合规或其他考量将该笔款项

包装为借款的,则需明确企业有权随时要求受托人归还借款。

3.控制权的归属与行使

控制协议应明确受托人作为股东和/或董事对境外主体的控制权最终归企业享有,受托人的任何决定均应取得企业的授权。控制协议还应约定企业行使对境外主体控制权的方式和受托人采取相应行动的期限。

4.受托人的报酬

为明确双方委托法律关系的定性,符合“衡平”原则的要求,企业应主动将向受托人支付报酬的标准和方式写入相应协议。

5.解除协议的安排

控制协议应提前约定解除整套协议文件的条件和程序。对于企业而言,应明确解除可以是无理由的,且程序应尽量简单,仅需通知即可,以便未来能够方便快捷地调整海外架构。对于受托人的解除条件则应在当地法律允许的前提下尽量难以达成,例如即使企业违约受托人也需进行催告而无效后才可解约,还要设置供企业找到新受托人的过渡期。解约后,应对受托人需要协助办理的变更登记等事项进行详细的约定,确保后续工作的顺利开展。

6.违约责任

违约责任是控制协议的重要条款,应明确受托人未能遵守控制协议应承担的责任。违约责任不能大而化之,而需要针对不同的情形约定不同的违约责任,确保在填平损失的基础上对于受托人的违约行为产生威慑作用。

(三)境外主体设立

协议签订完成后,即可以受托人的名义设立境外主体。在设立境外主体时应注意,最好不要直接使用受托人设立的境外主体作为实际的运营主体,而应在其下再设子公司,以规避风险,同时便利未来可能进行的交易。

二、以协议控制模式设立境外主体的优势与不足

(一)优势

1.成本更加低廉

企业选择协议控制模式的最主要理由是其成本较低,这既包括显性的金钱成本,也包括时间、精力等隐性成本。相比后文将介绍的信托模式,协议控制模式涉及的人员和法律层级都更少,法律关系相对也较为简单,相比信托公司的收费,单个受托人的报酬也更低,因此实施时的综合成本更低廉。

2.信息更加隐蔽

协议控制模式是完全的民事交易安排,交易内容本身无需任何行政机关的行政许可或行政登记,成立的企业在主管机关眼中是纯粹的受托人国籍地企业。在对于企业的实际控制权没有强制披露要求的国家,协议控制模式最有利于隐藏企业境内外主体间的联系,只要企业

自身及受托人做好保密工作,各方的关系就没有泄露的风险。

(二)不足

1.一旦被发现仍无法规避风险

为应对中国企业可能出现的规避美国管制措施的行为,美国针对中国的各项政策往往将“控制”列为重要的识别标准,制裁或出口管制规制的企业控制的主体往往也是规制的对象。协议控制模式无法切断境内企业对境外主体的控制,也就使得一旦被发现,协议控制模式就无法实现其希望达到的风险隔离的作用。

2.东道国法律认可程度有风险

为维护本国法律的权威,各国对于违反或故意规避当地法律的合同一般认定为无效。例如,印尼、泰国、越南等大部分东南亚国家对于外资进入都设置了严格的审查程序,为防止外国投资者规避审查,无论是立法还是实践都禁止当地居民为外国投资者直接在当地代持股权,在泰国违规代持的外籍股东和泰国公民甚至会面临三年以下的刑事处罚。如果企业设置的协议控制安排与当地法律存在不符之处,也可能导致代持行为因违反东道国法律而无效,这将给企业海外资产安全和业务发展带来毁灭性的打击。

3.资产安全风险大

协议控制模式决定,在公司登记等权利外观上均以受托人为权利人。背信的受托人完全可以在企业不知情的情况下按照自己的意愿转让、抵押境外主体的股权,即使受托人没有违约的主观意愿,相应权益也可能由于受托人债权人强制执行、受托人离婚、受托人死亡后发生继承等超脱受托人控制的原因发生变动。与受信托法保护的信托模式不同,此时企业将只能在东道国发起漫长的司法程序追索自己的权利,即使经过旷日持久的诉讼能够胜诉,此时境外业务也将受到严重影响甚至无以为继。

三、协议控制模式对企业在中国上市的影响

如前所述,协议控制模式存在较大的资产安全风险,且风险可能传导至投资人,因此在上市公司的领域一般受到信息披露方面的要求;但是,协议控制模式在被发现后即无法实现风险规避目的,因此其本质与上市存在一定冲突,本章将探讨相应问题。

(一)中国的上市公司监管要求

1.协议控制披露的必要性

无论是拟上市公司还是已上市企业均需遵守《证券法》第78条规定的信息披露义务。如前文所述,一旦企业为上市目的,公布其与境外主体间的控制关系,协议安排也就失去了风险防范的作用。那么,企业在境外作出的协议控制安排是否属于必须披露的范围?

答案是肯定的。证监会2023年发布的《公开发行证券的公司信息披露内容与格式准则第57号——招股说明书》第三十一条规定,发行人应简要披露重要子公司及对发行人有重大影响的参股公司情况,主要包括……股东构成及控制情况……发行人应列表简要披露其他子

公司及参股公司情况,包括股权结构、出资金额、持股比例、入股时间、控股方及主营业务情况等。以上规定已充分说明,无论是“重要子公司”还是“其他子公司”,其股权安排和持股情况都是必须披露的内容。企业需要注意,如果存在上市计划或属于上市公司,则需要披露其协议安排的情况。

2.协议控制是否必须解除

《首次公开发行股票注册管理办法》第十二条第(二)项要求“发行人的股份权属清晰,不存在导致控制权可能变更的重大权属纠纷”,《监管规则适用指引——关于申请首发上市企业股东信息披露》第一条则要求“发行人历史沿革中存在股份代持等情形的,应当在提交申请前依法解除”。由于代持等协议安排对公司控制权造成较大隐患,一般禁止上市公司自身出现股权代持的情形。但是,上市主体境外子公司的股权是否能够由第三方代持,是否必须解除?

从案例来看,答案是否定的。上海港湾(605598)在上市过程中披露了其海外子公司的代持,其中菲律宾港湾存在代持的原因是“当地法律对董事及股东组成有所限制”。上海港湾聘请的菲律宾律师事务所指出《菲律宾公司法》规定,公司至少要有5名董事,且董事必须至少持有公司1股股份,因此由一名上海港湾中国籍员工、一名新加坡籍自然人、三名菲律宾自然人作为菲律宾港湾董事并持有菲律宾港湾股份,但上海港湾的子公司“新加坡港湾一直实际控制菲律宾港湾的全部投票权并享有100%收益权”,形成了事实上的代持关系。为保证菲律宾港湾持续符合当地法律,在上海港湾聘请的菲律宾律师事务所出具的法律意见书保证相应情况合规稳定的前提下,上海港湾保持了菲律宾港湾的代持结构并完成了IPO。

(二)香港的上市公司监管要求

1.协议控制的有效性

香港法律原则上不禁止对公司进行协议控制。公司的协议控制按照香港法律被识别为信托关系,受到衡平法和信托法的双重调整,对于权利人而言较内地受到更有力的保护。对于上市公司而言,香港联交所也不要求拟上市主体解除现存的代持或类似安排。例如,鼎丰股份上市前的全部股份均由非实际权利人代持,且该种代持系出于便利业务发展的考虑,在法律上并无解除的障碍,但鼎丰股份仍然在维持该种代持的情况下成功完成了港股IPO。

2.协议控制的合规要求

协议安排必然涉及公司的控制权,香港对于此种情形为上市公司和非上市公司设置了不同的条件。对于注册地在香港,采取协议安排的未上市公司,香港法律要求置备重要控制人登记册(Significant Controllers Register,简称SCR),载明公司的重要控制人以备执法机关核查,SCR的内容仅可由香港司法机关查阅,不会向公众披露。港股上市公司则无需履行SCR义务,这是因为上市公司受有强制的信息披露义务,本就需要向公众披露其包括实际控制人在内的控制权情况。

第三篇 以信托模式设立境外主体

一、以信托模式设立境外主体的优势与不足

(一)以信托模式设立境外主体的优势

1.信托法律更有助于保障委托人/受益人权利

企业设立境外信托的目的地一般有关于信托的专门立法,此类立法往往重视保护委托人/受益人的合法权利。以新加坡为例,该国是普通法系国家,其信托制度起源于英美法。首先,在财产权制度上,其沿用了英美法的所有权二分法,认为虽然为使信托财产独立于委托人的财产,受托人能够享有法律所有权(Legal Ownership)衡平所有权,但受益人才享有衡平法所有权(Equitable Ownership)。也即,受托人享有的所有权能够使得受托人能够为管理目的自行行使对信托财产的处分权(而非基于代理),但其所有权又不能对抗受益人财产上的所有权,使受益人的权益得到保护。相比协议控制模式下出于意思自治的协议安排,这种法律上的制度设计无疑更具稳定性,也就更有利于保护委托人/受益人的合法权益。

其次,在履职过程中,新加坡《受托人法》的第一条实质性内容(第3A条,此前内容分别为法律简称、适用范围和定义)还规定了受托人的法定注意义务,即要求受托人在行使权利和履行义务时应尽到合理的注意义务,以保护委托人/受益人。

香港《受托人条例》还特别列明,信托公司的任何董事、高级人员或受雇人,如故意及意图欺诈,而忽略在公司的簿册内记入其职责上须予记入的记项,记入或教唆他人记入虚假记项,或签署或展示任何虚假文件的,都属于刑事犯罪,可依法对此种行为进行公诉。香港对于信托中背信和规避监管行为的刑事立法对于受托人具有更强的威慑作用,能够更加有力地保护受托人/受益人的权益。

2.投资路径更隐蔽

信托的另一大优势是其投资的路径更加隐蔽。近年来,出于打击洗钱、防范偷逃税款等目的,许多政府逐渐将信托不需进行任何注册、登记、备案或类似程序的规定改为了需向特定机关进行披露,或需置备最终受益人名册以供核查。但是为维护信托的保密性,此类法律往往同时注明,关于信托的登记信息不向公众或属地执法、司法机关外的第三方公开,能够在一定程度上保障信托的秘密性。

3.风险隔离更有效

信托结构能有效实现财产和风险的隔离,确保信托财产独立于委托人、受托人和受益人的其他资产。在制度设计上,信托一经设立,即在观念上认为信托财产不再是委托人的财产,受托人或受益人对其也不享有完全的所有权,这与协议控制模式下财产权益由委托人或受托

人一方单独持有的情况形成鲜明对比。此时,无论是委托人、受托人还是受益人的债权人,在与信托财产没有其他关联的情况下均无法主张信托财产的所有权;相应地,信托财产发生的债务问题,在委托人、受托人和受益人没有过错的情况下,也不会波及前述各方,能够实现较好的“防火墙”效果,保障企业境内外资产的安全。

(二)以信托模式设立境外主体的不足

1.设立成本更高

以信托模式设立境外主体的高成本主要体现在时间和资金两方面:

在时间成本上,信托的设立程序较为复杂,包括选择受托人、起草信托协议、设立信托账户、转移信托财产等环节,往往需要数月时间才能完成。而签订控制协议、设立一个普通的公司所需要的时间则相对较短,相比之下信托模式的时间成本极高,可能不适用于急于开展海外业务的企业。

在资金成本上,设立信托的花费也较高,可能的花费包括律师费、受托人服务费和信託管理费,信托运营中还可能产生审计费等。此外,部分法域还需支付额外的税务成本。信托是一项较为专业的事务,著名的信托目的地往往已产生较为明确的业务模式和链条,形成了较高的门槛,这也为专业服务机构收取的较高费用奠定了基础。相比之下,协议控制模式仅需签订协议并设立公司,其成本非常有限。

2.信托本质与管理要求可能存在冲突

信托的本质是将财产管理权交予受托人,但这种安排可能与委托人实际控制企业的需求产生冲突。在新加坡等部分法域,受托人有管理和运用信托财产的法定义务,必须独立决策,遵循信托协议的规定,而不允许委托人或受益人决定信托财产的处分。然而,在利用信托实现风险隔离的场合,委托人却往往希望能够对信托主体及其投资行为行使股东和董事权利,进行实际控制,这与信托的独立管理原则产生冲突。这种制度上的不协调,容易导致企业在



实际操作中的困境。即使是在如开曼这类允许委托人保留部分权利的司法辖区,保留权利的内容也是有限的,而且委托人在行权时也应注意克制。一旦信托被认定为虚假信托,可能导致信托自始无效,届时不但可能需要补缴期间享受的税收优惠,还可能陷入争夺信托财产所有权的尴尬境地。

二、以信托模式设立境外主体的基本路径

(一)寻觅合适的受托人

在信托模式下设立境外主体,选择合适的受托人至关重要。受托人不仅是信托财产的管理者,还承担着法律和道德上的责任。一般而言,除专门面对不特定多数人从事信托服务的持牌信托机构外,法律也允许具有信托需求的企业设立专门针对特定客户的私人信托机构,二者各有其优劣。

1.持牌机构

持牌信托机构通常是受当地金融监管机构监管的专业公司,如银行附属信托公司或独立的信托公司。这些机构具有丰富的信托管理经验、专业团队和规范的运营流程。其优点在于此类持牌机构受严格的法律监管,信托管理更具透明度和合规性。例如,新加坡金融管理局(Monetary Authority of Singapore, MAS)对信托公司实施严格的监管要求,确保受托人履行法律义务,保障委托人利益。持牌机构还提供专业的财务、法律、税务等一站式服务,有助于企业更好地进行资产管理和风险隔离。

持牌机构的缺点在于其往往收费较高,且由于其合规性要求较强,决策和执行过程可能相对缓慢,影响企业灵活应对市场变化。此外,持牌机构倾向于标准化的信托服务,难以满足委托人定制化的需求。尤其是在企业以信托模式出海的场合,持牌机构可能出于风险控制和避免纠纷的考量无法为出海企业提供服务。

2.私人信托机构

私人信托机构或个人受托人通常由家族成员、亲友或私人信托顾问担任,灵活性较高,且能够提供个性化的服务。私人信托机构的灵活性和低成本是其主要优势,委托人可以与受托人直接沟通,快速决策。信托管理更具私密性,特别适合需要高度保密的家族企业或私人财富管理需求。例如,在开曼群岛的私人信托安排中,由于不受严格的持牌监管,私人受托人可以提供更灵活的信托结构。但是,私人信托机构通常缺乏持牌机构的专业性和风险防范机制,尤其是在处理复杂的跨境法律和财税问题时,容易出现管理不善的情况,可能给出海企业造成比较严重的损失,严重时甚至会威胁信托架构的有效性。此外,私人受托人因未受严格监管,也可能存在法律和道德风险,难以充分保障委托人的权益。

(二)信托文件签署与资产转入

信托文件的签署和资产转入是信托模式设立的关键步骤,直接影响信托安排的合法性和有效性。

1.信托文件签署

信托文件是信托关系的核心法律文件,包括信托协议、受托人声明、资产转移文件等。信托文件应详细约定信托财产的管理、分配、变更和终止等条款。香港《受托人条例》、新加坡《受托人法》和开曼《信托法》均要求信托文件必须明确受托人的权利和义务,防止管理上的随意性和法律纠纷。

2.资产转入信托

签订信托文件后,委托人需将境外主体的股权或其他资产转移至信托名下完成信托设立。资产转移过程需遵循信托设立地的法律规定,并确保合法合规。信托财产转入后,委托人不再直接拥有这些资产的法律权利,而只能在法律允许的范围内,通过信托协议间接控制和管理这些资产。

3.法律和税务合规审查

在资产转入信托前,应进行全面的法律和税务合规审查,确保信托结构符合境内外法律要求。特别是在涉及多重税务管辖区时,合理的税务筹划至关重要。新加坡、香港等地的信托法律通常允许信托资产的跨境转移,但仍需谨慎处理税务合规和信息申报问题。

(三)境外主体设立

信托模式的关键步骤之一是设立境外主体,即由受托人利用受托财产成立境外公司。境外公司既可以成立在信托设立地,也可以设立在信托设立地以外的国家和地区,企业可以综合信托和外商投资领域的税收政策、法律环境、企业治理、信息披露要求等因素选择合适的设立地和注册形式。在此阶段中,还可以通过公司治理设计和董事等关键人员的选择实现对境外投资主体的控制。

三、以信托模式设立境外主体的风险及应对

(一)受托人的信誉风险及应对之策

在信托模式中,受托人作为信托财产的管理者,其信誉和能力直接影响信托的运作和安全性。在香港《受托人条例》和新加坡《信托法》中,受托人被要求忠实、勤勉地履行职责,但面对巨额的信托财产,受托人仍然可能发生道德风险,包括但不限于为自身或关联方牟利而损害信托财产、拒绝履行信托协议约定的义务、拒绝受托人依据信托协议发出的指示、擅自对境外公司作出较大的变动等。

拟出海企业可以采取以下方式,应对受托人信誉风险带来的威胁:第一是审慎选择受托人,应在选择受托人前进行背景调查并评估其过往的信托管理表现,优先选择信誉良好、专业能力强的对象作为受托人,在能够满足商业构想的前提下优先选择受到较强监管的持牌机构。第二是设置监督机制,通过信托文件规定定期的审计和报告机制,确保随时能够了解受托财产的情况,在必要时可以聘请独立第三方对信托管理进行监督。第三是明确法律义务和责任,企业可以在信托协议中详细列明受托人的管理责任和法律后果,以增强对受托人的约

束,并确保能够就受托人的失信行为得到救济。

(二)信托“被击穿”的风险及应对之策

信托“被击穿”风险是指在某些情况下,法院可能判定信托无效或“穿透”信托结构,直接认定信托财产为委托人个人财产,从而失去以上所述的风险隔离效果,甚至针对信托财产及其收益产生额外的信托。一旦出现与信托相关的诉讼,还可能由于法院或对方当事人公开案件情况,导致信托架构引起舆论关注,丧失其秘密性。此种情况集中体现在著名的“俏江南”创始人,张兰女士的信托被新加坡法院认定无效一案中。在该案中,张兰女士于库克群岛设计了信托,但实际装载信托财产的公司设立于英属维尔京群岛(BVI),该公司分别通过在两家新加坡银行开立的账户持有1.42亿美元现金。新加坡法院经审判认为,由于张兰女士体现出了对信托财产的较强控制力,实质上并未实现财产的独立性和管理的独立性,因此信托仅仅是她规避债务的工具。因此,法院判定信托无效,将信托财产视为张兰的个人资产用于清偿债务。此案非常生动地体现了信托的日常管理中不符合法律规定可能导致的严重后果。

为应对类似风险,受托人首先应在设立信托时,尽可能选择允许委托人留存管理权的东道国;其次,在订立信托协议时,应在法律框架内明确委托人的管理权限;再次,在信托的管理过程中,则要严格在法律允许和信托协议约定的框架内履行对信托的管理权限,实现控制与合规的平衡;最后,可以聘请独立的第三方进行合规审计,明确现有方式的合规性,及时弥补漏洞、规避风险。

(三)信托的税务合规风险及应对之策

虽然信托安排通常也被认为具有税务筹划的功能,但不同国家对信托的税务处理方式各异,跨境信托可能涉及多重税务管辖的复杂问题,尤其是以信托形式出海的情形下还要考虑到出海主体在运营过程中的税务筹划,这带来了更高的税务合规风险。具体而言,风险可能来自以下几方面:第一是税务居民身份认定,部分国家可能将信托视为本地税务居民,从而对信托收入征税,导致信托在受益人所在地、信托设立地、出海主体运营地产生三重甚至多重征税问题。第二是反避税条款,近年来,全球国际反避税合作加深,反避税规则日益严格,一些国家已出台针对信托的特别税务规定,例如澳大利亚即对利用信托形式将收益分配给受益人,但受益人又将收益变相返还给委托人的行为进行了特别规制,税率最高可达47%。第三是转让定价与受控外国公司(CFC)规则,英国、日本、德国等国家对外国信托实施受控外国公司规则,将信托的收入视为委托人的收入,防止其税务居民利用信托避税。

为应对以上风险,企业需在信托架构设计阶段即广泛征求涉及的各司法辖区专业人士的意见,防止信托设立完成后发现税务风险,产生额外成本;在信托运行中,还应定期审查信托的税务影响,核查信托的税务合规情况及相关税务法律的变动情况;企业还应定期履行各主管当局规定的信息披露义务,防止由于披露不合规受到处罚。

第四篇 主体设立中的税务因素

一、出海企业税务筹划的重点关注

(一)跨国税务架构设计

1.选择合适的税收管辖区

企业跨境选择合适的税收管辖区是一个复杂而重要的决策过程,涉及多个方面的考量。企业应深入研究目标税收管辖区的税收法规,包括所得税、增值税、关税等主要税种的规定,以及税收优惠政策和税收协定等。不同税收管辖区的税率水平可能存在较大差异,企业应选择税率相对较低且稳定的税收管辖区,以降低税负并提高盈利能力。同时,企业应根据自身的业务需求选择合适的税收管辖区。例如,如果企业主要从事大模型领域业务,可能需要选择对大模型行业有税收优惠政策的税收管辖区。税收管辖区的地理位置、物流成本和供应链效率也是企业需要考虑的因素。企业应选择交通便利、物流成本较低且供应链稳定的税收管辖区。

2.设立控股公司、子公司或分支机构

从税务的角度来看,如果企业在海外的东道国只有一个,通常只需设立一个海外控股主体;如果企业涉及多个东道国,特别是位于不同大洲,可能需要结合各东道国的税收规则和税收协定安排,考虑设立多个控股公司。常见的做法是,在不同大洲设立单独且并行的控股公司,还可以在這些控股公司之上设立更高层级的统一境外控股主体(例如,海外总部)。多层控股结构可以为集团在境外的关联交易定价、未来的退出和融资提供灵活性和税务优化的空间,同时也会增加持股结构的维护成本和管理复杂度。因此,企业需综合考虑税务效率、管理成本和未来发展战略,制定最合适的控股结构。

目前,在境外投资的公司几乎都设立子公司,不设立分公司。税收方面,以在美国投资为例,如果在海外设立经营实体业务公司,大多数投资者在美国选择设立子公司,第一,美国子公司自行申报纳税,自行申报其所得,因此一般而言,与分公司相比较,子公司披露母公司的财务信息一般少于分公司必须披露的有关母公司的财务信息。第二,子公司纳税申报表通常比分公司的纳税申报表简单。

3.利用税收协定降低双重征税风险

经营主体东道国与中国、控股公司所在国之间的税收协定(如避免双重征税协定、关贸协定等)对企业实现持股架构和供应链的整体税负优化至关重要。其中,避免双重征税的协定中要特别关注税收居民的认定、利润汇回的预提税、股权转让所得及常设机构、员工个税等条件。

(二)税务合规与风险管理

1.深入了解目标国家的税法规定

企业应了解目标税收管辖区的税务监管环境,包括税务机关的执法力度、税收政策的稳定性和透明度等。选择税务监管环境良好、政策稳定的税收管辖区有助于降低税务合规风险。企业应充分利用各国签订的税收协定,避免双重征税。在选择税收管辖区时,优先考虑已与中国签订税收协定且协定内容有利于企业的国家。同时,企业应关注国际税收合作的发展趋势,特别是税基侵蚀和利润转移项目的成果和各国对跨国企业的税务监管要求。选择国际税收合作紧密、税务监管体系完善的税收管辖区有助于企业更好地应对跨国税务挑战。

2.建立健全税务合规体系

企业应根据各国税收法律法规,结合企业实际情况,制定详细的税务合规政策,明确税务筹划、申报、缴纳等环节的具体要求。优化税务管理流程,确保税务活动的高效、准确和合规。包括税务登记、发票管理、纳税申报、税款缴纳、税务自查等环节。建立税务风险预警机制,对潜在税务风险进行识别、评估、监控和应对,确保税务风险的及时发现和有效控制。增强员工税务意识,通过内部培训、外部讲座等方式,增强员工的税法意识和税务合规意识,确保员工了解并遵守税收法律法规。

3.定期进行税务风险评估与应对

企业应加强税务专业人才的培养和引进,建立专业的税务管理团队,提高企业的税务管理水平和合规能力,定期进行税务自查。利用现代信息技术手段,建立税务信息系统,实现税务数据的自动化处理和分析,提高税务管理的效率和准确性。确保税务数据的安全性和保密性,防止数据泄露和滥用,保护企业的合法权益。与各国税务机关建立良好的沟通机制,及时



了解税收法律法规的变化和税务机关的监管要求,确保企业的税务合规活动符合税务机关的期望。在税务机关进行检查时,企业应积极配合,提供必要的资料和说明,确保检查的顺利进行。同时,通过检查发现的问题,及时整改和完善税务合规体系。

二、特定国家/地区的税收管理规定

(一) 美国

1.美国联邦税与州税的协调处理

在美国,联邦税与州税的协调处理是一个复杂而重要的议题。联邦税由联邦政府征收,主要包括联邦个人所得税、公司所得税、消费税等。联邦个人所得税税率根据收入水平而定,分为多个档位,税率从低到高不等。州税由各州政府征收,主要包括州个人所得税、销售税、财产税等。各州的税率和征税方式因州而异,税率数值也有较大差异。

在联邦税与州税协调处理方面,需注意以下三方面着手:(1)避免重复征税。联邦政府和各州政府实行税收协调机制,以避免对同一税源进行重复征税。纳税人在缴纳联邦税时,可以申报已经支付过的州税,以得到相应的抵免减免。(2)州税抵扣联邦税。在填报联邦所得税申报单时,纳税人可以选择标准抵扣或逐项抵扣。如果选择逐项抵扣,纳税人可以把支付的州所得税作为抵扣项,这一选项对于那些居住在州税较高的州的纳税人尤其有利。但需要注意的是,州所得税抵扣可能会使一些纳税人的应纳税所得增加,从而受到替代最低税(AMT)的影响。(3)税收抵免。税收抵免是联邦政府用来协调州地政府税制的一种方法。各州之间为吸引资金,可能在税率上展开竞争。而通过税收抵免,可以协调各州的税制,避免不必要的竞争。

2.海外税收抵免与豁免政策

海外税收抵免(Foreign Tax Credit, FTC)是美国税法中的一项重要规定,旨在减轻美国公民和居民纳税人因在海外赚取的收入且在海外收入来源地已缴纳税款,在回美国后再次面临美国国内的征税压力。它允许纳税人在计算美国联邦税时,抵免其在海外已缴纳的税款。FTC的抵免规则的核心要点是允许纳税人将在海外合法且被美税务机关认可的已缴纳的所得税用于抵免其在美国的所得税。但FTC的抵免额不能超过同一收入在美国应纳税额的计算结果。首先,纳税人需要确定在美国海外支付的税种是否符合FTC的抵免资格。只有所得税和某些非自愿性的税款(如房产税等)可能符合条件。消费税、增值税、关税和社会保障税等通常不符合抵免条件。如果美国纳税人是一个美国海外共同基金或其他受监管投资公司的股东/成员,且该基金选择将信用额传递给其股东,该纳税人可以根据其在基金支付的海外所得税的份额申请这项税收抵免。该纳税人应该从共同基金那里收到一份Form 1099-DIV表格或类似声明,显示相关海外收入份额以及其支付的在海外税款份额,否则无法作为FTC在其美国税务申报时进行抵免。同时,税款必须是合法和实际的外国纳税义务。合格的海外税款需要是纳税人在一个纳税年度支付或应计的合法和实际海外纳税义务。符合抵免条件的海外税款金额必须减去外国政府退还的外国税款。

(二) 欧盟

1. 欧盟内部税法的统一性与差异性

欧盟内部税法的统一性与差异性并存,这是由欧盟的特殊政治经济结构和成员国的主权独立性共同决定的。欧盟内部税法的统一性主要表现在以下三方面:法律基础统一,欧盟所得税法是协调成员国所得税法的欧共体基础条约、二级立法以及欧洲法院判例的总称。欧盟所得税法依托于共同体基础条约而存在,如《欧洲共同体条约》第 293 条(原第 220 条)要求成员国应彼此谈判,以确保消除共同体内的双重征税。税收协调统一,欧盟致力于协调各国税法,在欧盟层面制定统一的税收规则来消除欧盟内跨境交易的障碍。例如,欧盟先后出台了利息和特许权使用费指令、企业并购指令、母子公司指令,旨在消除企业在欧盟内跨境商业活动的税收障碍,维护统一市场。税收争议解决机制统一,欧盟实行了有效的税收争议解决机制,如相互协商程序和仲裁等,以统一规则解决成员国间的跨境税收争议,保障法律确定性,维护统一市场的运行。同时,欧盟各成员国的税法差异性确实存在,这些差异主要体现在税率、税收优惠政策、税务申报和缴纳流程等方面。以下是一些具体的例子:

(1) 税率差异

增值税(Value Added Tax, VAT): 卢森堡的增值税标准税率是 17%,而瑞典的标准税率则高达 25%。德国的一般商品增值税率为 19%。

企业所得税:德国和西班牙的企业所得税率为 16%,而瑞典和丹麦的税率则较高,达到 25%左右。葡萄牙对公司所得税设有临时抵免政策,如对 2013 年内的投资给予不超过投资额的 20%或 100 万欧元的临时公司所得税抵免。

(2) 税收优惠政策差异

研发优惠:多数成员国通过税收优惠促进私人的研发投入,但具体的优惠政策和力度有所不同。例如,瑞典下调了雇主为研发人员缴纳的社保税,而意大利对招聘研发活动中的高技术人员给予税收抵免。

创业投资优惠:一些成员国如爱尔兰、西班牙和葡萄牙实施优惠以促进利润再投资,特别是针对小企业。瑞典对天使投资实施新的税收优惠,即个人购买中小企业股份可以按购价的一半从其当年资本净利得中扣除。

(3) 税务申报和缴纳流程差异

申报周期:大多数欧盟国家要求企业定期提交增值税申报表,但申报周期有所不同。例如,德国要求企业每月申报增值税,而法国则允许按季度申报。

申报方式:一些国家要求电子申报,而其他国家则接受纸质申报。欧盟的“一站式”(One-Stop Shop, OSS)制度旨在简化增值税申报流程,但 OSS 制度的具体规则和适用范围在不同国家之间有所不同。

税收抵免和退税规定:各国对于税收抵免和退税的规定也存在差异。例如,企业在其他国家支付的增值税可能可以在本国申报抵免,但具体的操作和要求在各国之间存在差异。

综上所述,欧盟各成员国的税法差异性主要体现在税率、税收优惠政策以及税务申报和缴纳流程等方面。这些差异反映了各国经济发展状况、财政需求以及税收政策的不同。因

此,在欧盟内部进行跨境贸易或投资时,需要充分了解并遵守各国的税法规定。

2.跨国企业合并与重组的税务处理

欧盟对于跨国企业合并的税务优惠政策,主要体现在以下几个方面,这些政策旨在促进企业的合并与重组,同时确保税收制度的公平性和效率:

(1)延期纳税规定

欧盟通过相关指令,对适用于转让给常设机构的部分资产有关的被转让资产的资本收益,允许延迟至该资产实际处理后才课税。这种延期纳税的制度,实际上为跨国企业合并提供了税收优惠,因为它允许企业在合并过程中避免立即承担税负。

(2)合并企业亏损抵扣的继受规定

在欧盟范围内,如果跨国企业合并发生在成员国之间,并且接收公司所在国采用允许接收公司接收转让公司的税收上尚未了结的亏损的条款,那么该成员国应将这些条款的应用扩大到包括由位于其领土内的接收公司常设机构接收的亏损。这一规定有助于降低合并后企业的税负,因为它允许企业利用转让公司的亏损来抵扣未来的盈利。

(3)税收免除规定

在某些情况下,欧盟允许接收公司在注销其控股所得到的收益时不应纳税。这通常发生在接收公司拥有转让公司的资本时,特别是当接收公司在转让公司的资本方面的控股不超过一定比例(如25%)时,各成员国可以不执行上述应纳税的规定。这为跨国企业合并提供了额外的税收优惠。

(4)全球最低税制度

2024年1月1日,欧盟关于企业税的新法规正式生效。这一新规生效后,对在欧盟成员国的跨国公司实行15%的最低有效税率,主要目的是打击跨国企业在欧盟市场各国转移利润以逃税避税的行为,它要求跨国企业无论在哪个辖区获得的经营利润,都需缴纳至少15%的税。实施方式由规定的辖区依据收入纳入规则(Income Inclusion Rule,IIR)或低税支付规则(Undertaxed Payments Rule,UTPR)对实际税负(有效税率)低于15%的低税所得征收补足税。这两个规则的实施有一定的顺序,即收入纳入规则要优先于低税支付规则。全球最低税规则适用于欧盟的跨国企业集团和大型国内集团,其年财务收入合计超过75亿欧元(或7.5亿欧元,具体根据法规的不同解读而有所差异)。

虽然这不是直接针对跨国企业合并的税务优惠政策,但全球最低税制度的实施对跨国企业合并的税务筹划产生了重要影响。从2024年起,欧盟对跨国公司征收至少15%的税收,这一制度有助于平衡各国之间的税收竞争,减少跨国企业通过税收筹划将利润转移到低税率国家的行为。在一定程度上,它促使跨国企业在合并时更加关注税务筹划的合规性和有效性。

(5)特定准备金移转规定

欧盟允许在特定情况下,专门有转让公司设立的准备金得到部分或全部免税移转给接收公司。这些准备金可由位于转让公司成员国的接收公司常设机构按照同一免税额予以接转。这一规定有助于降低合并后企业的税负,因为它允许企业利用现有的准备金来减少未来的税收支出。

综上所述,欧盟为跨国企业合并提供了多种税务优惠政策,这些政策旨在降低企业合并

过程中的税负,促进企业的健康发展。然而,企业在利用这些优惠政策时,也需要遵守欧盟及成员国的相关税收法规和规定,确保税务筹划的合规性和有效性。

(三)新加坡

1.低税率与税收优惠政策的利用

新加坡的税收制度以属地原则为基础,即公司和个人在新加坡发生或来源于新加坡的收入,或在新加坡收到或视为在新加坡收到的收入,都属于新加坡的应税收入,需要在新加坡纳税。相反,如果收入来源于新加坡境外,并且不是在新加坡收到或视为收到,则不需在新加坡纳税。这一原则为国际企业在新加坡的运营提供了极大的便利。

(1)企业所得税

新加坡的企业所得税税率为17%,相较于其他国家如中国的25%,具有明显的税率优势。此外,新加坡还为企业提供了一系列税收减免和优惠政策,以降低企业的税负。例如:

初创企业税务减免:新成立的新加坡公司在首三个税务年度内可享受高额的税务减免。首10万新币以内的应税收入减免75%,相当于税率4.25%;下一个10万新币的应税收入减免50%,相当于税率8.5%;超过20万新币的应税收入部分按正常税率17%征收。

部分免税政策:所有新加坡公司每年在利润的前1万新币内可享受75%的减免,下一个19万新币的应税收入减免50%,超过20万新币的部分按正常税率征收。

企业所得税回扣:为帮助企业应对成本上升和经济不确定性,新加坡政府还为企业提供企业所得税回扣,具体回扣率根据政府年度预算公告确定。

(2)海外收入免税

新加坡对从海外获得的资本收益、股息或收入免税,这意味着在新加坡注册的公司无需为其海外分支机构的利润或股息缴纳所得税。

(3)消费税(Goods & Services Tax, GST)

新加坡的消费税是对进口商品以及新加坡几乎所有商品和服务供应征收的广泛消费



税。目前GST税率为9%。对于年收入超过100万新币的公司,必须注册GST并定期向税务局申报。GST豁免适用于大多数金融服务的提供、数字支付代币的供应、住宅物业的销售和租赁以及投资贵金属的进口和本地供应。

(4)个人所得税

新加坡的个人所得税采用累进税率制,税率保持在0–22%之间。居民个人的应税收入在扣除支出、捐款和税收减免后,按累进税率缴纳所得税。首2万新元的应课税收入以零价值征税。非居民个人则根据停留时间和收入类型适用不同的税率,一般为15%或累进税率中的较高者。新加坡的个人所得税还设有一些税前扣除项,如个人养老金、医疗保险、教育支出等,可减少个人所得税的负担。

为更直观地展现我国与新加坡税收制度的不同,本文在本部分就中新两国常见税种税率进行对比如下:

中国	新加坡
最高企业所得税税率(%)	
25	17
综合个人所得税税率(%)	
45	24
增值税标准税率(%)	
13、9或6,具体取决于商品和服务的类型	商品及服务税:9
预扣税税率(%) (股息/利息/特许权使用费)	
居民: 不适用; 非居民: 10/10/10	居民: 不适用; 非居民: 0/15/10
总体企业资本利得税率(%)	
资本利得需缴纳正常企业所得税税率	不适用
总体个人资本利得税率(%)	
20	不适用
总体净财富/价值税率(%)	
不适用	不适用
总体遗产税率(%)	
不适用	不适用
总体赠与税率(%)	
不适用	不适用

来源: <https://taxsummaries.pwc.com/>

(5) 双边税收协定的签订与执行

作为金融中心,新加坡与多个国家或地区签订了全面性或有限性的双边或多边税收协定,因此,海外公司注册在新加坡,一般都不会面临双重征税问题。具体而言:

新加坡共与约 100 个国家和地区签订了 107 份税收协定,其中包括美国、中国、马来西亚、印度、日本等 97 个避免双重征税协定(Double Taxation Avoidance Agreements,DTA),8 个有限课税协定(Limit DTA)以及 2 个信息交换安排(EOI Arrangement),这意味着符合条件的“新加坡税收居民”在与这些国家进行跨国交易时,可以避免在两个国家或地区被双重课税,或可以减少双重课税的额度。

以我国与新加坡签署的《中华人民共和国政府和新加坡共和国政府关于对所得避免双重征税和防止偷漏税的协定》为例,前述协定于 1986 年 4 月 18 日由中国政府与新加坡政府正式签署,2007 年 7 月 11 日中国政府与新加坡政府签署新的政府间对所得避免双重征税和防止偷漏税的协定(以下简称“2007 年协定”)及其议定书,2009 年 8 月 24 日双方签署了 2007 年协定的第二议定书,2010 年 7 月 23 日双方签署了 2007 年协定的第三议定书。2007 年协定及其议定书以及第二议定书、第三议定书分别于 2008 年 1 月 1 日、2009 年 12 月 11 日、2010 年 10 月 22 日生效。四份文件共同构成了中新税收协定的规范总体,不仅包括了实体性税收规范,而且包括程序性税收规范。

以 2007 年协定中有关“营业利润”的规定为例,中新双方中一方的企业若在另一方拥有常设性机构(Permanent Enterprise)并通过该常设性机构从事营业活动,则由该营业活动所获得的利润可由另一方的国家征收所得税。有关条款规定在计算利润时,由企业总部向常设性机构所收取的权利金、特许或专利费、佣金、管理费或利息(除非是偿还实际代付的开销包括权利金,利息和其他类似的收费)都不得加以扣除。常设性机构的定义包括分行、办事处、工厂、车间、矿井;超过 6 个月的建筑工程或建设,装配与装置的工程项目,和超过 6 个月的咨询服务。

新加坡以其低税率、简单税制和广泛的税收优惠政策,成为众多国际企业和投资者的首选之地。无论是初创企业还是成熟企业,都能在新加坡找到适合自己的税收优惠政策,降低税负,提升竞争力。

(四) 沙特阿拉伯

金砖国家领导人第十五次会晤宣布金砖国家扩员,将新增埃及、埃塞俄比亚、伊朗、沙特阿拉伯、阿联酋加入金砖合作机制。随着不断扩大与金砖国家贸易往来,沙特阿拉伯成为企业出海的主要目标国之一。

扎卡特、税务和海关总局(Zakat,Tax and Customs Authority)为沙特税务主管部门。沙特的税收法律体系规定对沙特籍居民征收扎卡特税、对非沙特籍居民征收所得税。自 2018 年起,沙特与海合会成员国共同行动,开征增值税。目前征收的其他税费还有消费税、关税、土地税、人头税和房地产交易税等。沙特税收体系中不仅有沙特居民的概念,还有沙特籍的概念,两者区别在于:前者用于区分国内税与国外税的纳税义务,后者用于区分在沙特国内税中所得税与扎卡特税的纳税义务。

沙特所得税法(王室法令第 3321 号)是沙特关于所得征税的统一税法,沙特国内不区分企业所得税与个人所得税,该税法将企业利润、个人所得、股息及资本利得等收入都作为一般性所得统一课税。对于企业而言,居民企业判断标准为一个纳税年度内满足以下两个条件中的任意一个即被视为沙特居民企业:(1)该企业根据沙特法律注册成立;(2)该企业的实际管理机构位于沙特境内。

税率设置方面,对于居民企业、非沙特籍的居民自然人及通过常设机构从事商业活动的非居民企业或者非居民自然人,标准所得税税率为 20%。弥补亏损方面,当年亏损可以在在以后年度计算计税依据时进行弥补,直到亏损完全弥补为止,每年允许扣除的最高限额不得超过年度应税所得额的 25%。

股息方面,沙特居民企业从其他企业(包括居民企业和非居民企业)取得的股息,在满足以下两个条件的情况下免税:①股息接收方拥有被投资企业 10%(含)以上的股份;②股息接收方持有被投资企业股份 1 年(含)以上。

预提所得税方面,沙特居民企业,或非居民企业在沙特的常设机构,在对外支付来自沙特境内的款项时都应支付预提所得税。具体税率如下:

付款性质	预提所得税税率(%)	
	非关联方	关联方
股息	5%	
利息	5%	
特许权使用费	15%	
管理费	20%	
租金	5%	
机票费、空运或海运费	5%	
保险或再保险费	5%	
技术或咨询服务费	5%	15%
国际电信服务费	5%	15%
其他付款	15%	

实务中,为促进海外成员企业更好发展,“走出去”企业中国母公司可能会向海外成员企业提供专利、商标等使用权许可,并收取相应报酬,根据沙特所得税法,一般情况下特许权使用费的预提所得税税率为 15%,而根据中沙税收协定给予企业优惠待遇,“走出去”企业可以适用 10%的税率就取得的特许权使用费缴纳预提所得税。

境外投资审批 及境外融资架构

第二章

第一篇 中国企业境外投资的审批与监管

中国企业去境外投资设立公司，需要在商务部门、发展和改革委员会以及外汇管理部门完成相关备案/核准或登记手续(以下合称“ODI手续”)，中国企业在完成ODI手续后，可将资金投入境外子公司并开展运营。本篇主要从审批与监管角度展开介绍中国企业境外投资的具体流程。

一、商务主管部门备案（或核准）

根据商务部于2014年9月6日发布的《境外投资管理办法》(商务部令2014年第3号)规定，境外投资，是指在中国境内设立的企业通过新设、并购及其他方式在境外拥有非金融企业的所有权、控制权、经营管理权及其他权益的行为。

商务主管部门对境内企业的境外投资分别实行备案和核准管理。境内企业境外投资涉及敏感国家和地区、敏感行业的，实行核准管理，其他情形适用备案管理。实行核准管理的敏感国家和地区包括，与中国未建交的国家、受联合国制裁的国家；实行核准管理的敏感行业包括涉及出口中国限制出口的产品和技术的行业、影响一国(地区)以上利益的行业。对属于核准情形的境外投资，中央企业向商务部提出申请，地方企业通过所在地省级商务主管部门向商务部提出申请。

经商务主管部门核准或备案后，境内企业将获得《企业境外投资证书》，该证书是境内企业境外投资获得备案或核准的凭证，按照境外投资最终目的地颁发，有效期是2年。“最终目的地”指境内企业投资最终用于项目建设或持续生产经营的所在地，对于境内企业投资到最终目的地企业的路径上设立的所有空壳公司，商务主管部门均不予备案或核准。

如果有两个以上境内企业共同在境外进行投资的，通常由持股比例较大的一方在该方所在的商务主管部门办理备案(或核准)。如果两个境内企业持股比例相同，应当双方协商后由一方办理。

二、发改委备案（或核准）

根据国家发展和改革委员会(以下简称“国家发展改革委”)于2017年12月26日发布的《企业境外投资管理办法》(国家发展改革委令11号,“11号令”)规定，境外投资，是指中国企业直接或通过其控制的境外企业，以投入资产、权益或提供融资、担保等方式，获得境外所有权、控制权、经营管理权及其他相关权益的投资活动，包括但不限于：获得境外土地所有权、使用权等权益；获得境外自然资源勘探、开发特许权等权益；获得境外基础设施所有

权、经营管理权等权益;获得境外企业或资产所有权、经营管理权等权益;新建或改扩建境外固定资产;新建境外企业或向既有境外企业增加投资;新设或参股境外股权投资基金;通过协议、信托等方式控制境外企业或资产。

境内企业开展境外投资,应当履行境外投资项目核准或备案等手续。其中,涉及发改委11号令项下的敏感国家和地区,或涉及敏感行业的敏感类项目,应适用核准管理;非敏感类项目,则适用备案管理。发改委11号令项下的敏感国家和地区包括与我国未建交的国家和地区,发生战争、内乱的国家和地区,以及根据我国缔结或参加的国际条约、协定等,需要限制企业对其投资的国家和地区;敏感行业包括武器装备的研制生产维修,跨境水资源开发利用,新闻传媒,房地产,酒店,影城,娱乐业,体育俱乐部,及在境外设立无具体实业项目的股权投资基金或投资平台等。

根据11号令,境内企业应当在境外投资之前取得发改部门出具的项目核准文件或备案通知书,如未能取得有效核准文件或备案通知书的,外汇管理、海关等有关部门依法不予办理相关手续,金融企业依法不予办理相关资金结算和融资业务。核准文件和备案通知书有效期是2年。

如果有两个以上企业共同对境外主体进行投资的,通常由投资额最大的一方代表其他投资人共同申请办理。

三、外汇登记

根据国家外汇管理局(以下简称“外汇局”)于2009年7月13日发布的《境内机构境外直接投资外汇管理规定》(汇发〔2009〕30号)的相关规定,境内投资人境外直接投资获得境外直接投资主管部门(目前即商务主管部门和发改委)备案(或核准)后,应到所在地外汇局办理境外直接投资外汇登记。外汇局审核无误后向境内投资人颁发境外直接投资外汇登记证。根据《国家外汇管理局关于进一步简化和改进直接投资外汇管理政策的通知》(汇发〔2015〕13号,“13号文”),自2015年6月1日起,取消境外直接投资项下外汇登记核准行政审批,改由银行直接审核办理,国家外汇管理局及其分支机构通过银行对直接投资外汇登记实施间接监管。

投资人凭境外直接投资主管部门的核准文件和境外直接投资外汇登记证,在外汇指定银行办理境外直接投资资金汇出手续。外汇指定银行为境内企业办理境外直接投资资金汇出的累计金额,不得超过其事先在相关业务系统中登记的境外直接投资外汇资金总额。

中国企业如果要在海外设公司开展业务,则须完成全部ODI手续之后,才能合法合规地将资金投入境外公司并开展业务。

第二篇 搭建公司架构的类型与选择

一、公司架构的常见类型

公司架构存在不同的类型,若以融资主体和实际运营主体所在地的不同分类,可分为境内架构、红筹架构和境外架构。

(一)境内架构

境内架构即融资主体与实际运营主体均在中国境内的公司架构,通常融资主体与实际运营主体为同一主体。境内架构又分为内资架构及中外合资架构(以下简称“JV架构”)。内资架构项下融资主体的股东均为境内主体;JV架构下融资主体的部分股东为境外主体。特别是对于香港特别行政区、澳门特别行政区投资者在内地投资,也适用外商投资法律法规的监管。而台湾地区投资者在大陆投资,适用《中华人民共和国台湾同胞投资保护法》及其实施细则的规定,上述法律法规未规定的事项,也参照外商投资法律法规的监管。

(二)红筹架构

红筹架构即融资主体在中国境外,但实际运营主体在中国境内。红筹架构又分为大红筹架构和小红筹架构,大红筹架构下,融资主体一般被境内企业控制,小红筹架构下,融资主体一般被境内自然人控制。而红筹架构下,根据融资主体对实际运营主体的控制方式不同又分为股权控制型红筹架构和协议控制型红筹架构(即VIE架构)。股权控制即融资主体通过在不同国家或地区层层设立主体最终实现间接持有境内运营主体的股权;协议控制指在实际运营主体存在外资限制或禁止的情况下融资主体通过其控制的境内外商投资企业与境内运营主体签署一系列协议实现对实际运营主体的间接控制。该等协议包括独家购买权合同、独家服务和业务合作协议及股权质押合同等。

(三)境外架构

常见的境外架构是非中国籍自然人在海外设立公司,通过海外的融资主体进行融资,未来在海外上市,实际业务运营主体也在海外。目前市场上有一些计划主要在海外开展业务的大模型企业,创始人是非中国籍公民,会选择搭建境外架构,在海外开展业务,并接受海外投资人的投资。但如果创始人是中国籍自然人,从合规性的角度,创始人在海外设公司应进行37号文登记,所以即使公司主营业务在海外,基本上还是会选择搭建红筹架构。

二、选择公司架构的考量因素

以下四项考量因素,是决定搭建何种公司架构的核心考量因素。

(一)外资准入

如根据国家发展和改革委员会、商务部发布并不时更新的《外商投资准入特别管理措施》(“负面清单”),如实际运营主体所从事的业务落入负面清单中的外资禁止业务,则公司要么选择内资架构,仅接受人民币投资人的投资,且人民币投资人穿透后也不得存在外资成分,要么选择搭建VIE架构来接受美元投资人或人民币投资人的投资。VIE架构下的境外融资平台(惯常是一家设立在开曼群岛的公司)接受境外投资人的投资,设立在中国境内的、被境外融资平台协议控制的企业作为业务运营实体,该境内企业的股东无任何外资成分,以此来规避外资准入的限制。

(二)上市地

如公司拟在境外上市的(常见境外上市地包括美国、香港),则可以选择搭建红筹架构,以境外融资平台在境外上市,或在满足法律法规监管的前提下直接赴港上市。

(三)税务筹划

如公司有避税需求,则可以选择搭建红筹架构在开曼群岛(Cayman Islands)或英属维尔京群岛(British Virgin Islands,即BVI)设立公司来进行避税,开曼群岛和BVI作为避税地,一般不征收所得税、资本利得税、企业税、计提税或其他类似的税。

(四)主营业务开展地

如果公司的主营业务主要在海外开展,未来绝大部分收入来自海外,且海外的品牌知名度更高,在这种业务规划下,公司更适合搭建红筹架构或境外架构,在海外融资及上市。

在公司搭建红筹架构或境外架构后,公司仍然可以接受人民币投资人的投资,人民币投资人可以通过办理ODI手续的方式对境外融资平台进行投资。当然,美元投资人也可以在合规地完成外商投资手续后直接投资到中国企业。因此,企业不论是想拿美元投资人的钱,还是想拿人民币投资人的钱,不会单方面地实质影响公司架构的选择,应当综合考量各项因素后再选择适合自身情况的公司架构。

第三篇 搭建红筹架构的惯常操作步骤

中国企业进行境外融资并上市,最常见的公司架构是红筹架构。本篇主要介绍什么是红筹架构,以及最常见的红筹架构搭建流程。

一、大红筹和小红筹

(一)大红筹

大红筹结构,是指拟于境外资本市场上市的主体是境外注册的公司(常见的注册地如英属开曼群岛、中国香港、百慕大等地),但其主要业务、资产均来自其所控制的境内主体,而该境内主体的实际控制人为境内机构的结构。在实践中,除少数大型国有企业采用大红筹架构申请境外上市外,创业企业采用大红筹架构的几乎没有,本篇不作过多讨论。

(二)小红筹

小红筹结构,是指拟于境外资本市场上市的主体是境外注册的公司(常见的注册地如英属开曼群岛、中国香港、百慕大等地),但其主要业务、资产均来自其所控制的境内主体,而该境内主体的实际控制人为境内自然人的结构。

一般而言,搭建小红筹架构,主要是通过以下两种方式进行,(1)如该主体所处行业为外商投资鼓励行业,或者虽为外商投资限制行业但能够符合负面清单规定的限制性准入特别管理措施(比如满足外商投资比例要求并取得必要业务资质),且不存在其他法律法规的障碍,则一般搭建股权控制型小红筹架构,由境外控股公司实现对境内运营公司的间接控股;(2)如该主体所处行业为外商投资禁止行业,或属于外商投资限制行业并且不符合负面清单规定的限制性准入特别管理措施(比如不满足外商投资比例要求或未取得必要的业务资质),或存在其他法律法规障碍,则一般搭建协议控制型红筹架构(即常见的VIE架构),由境外控股公司通过协议控制的方式实现对境内运营公司的控制。

需特别注意的是,如境内民营企业拟于香港联交所上市,根据香港交易所上市规则,上市申请人仅可于必要的情况下以合约安排(即VIE架构)的方式解决中国大陆法项下的外资准入限制,否则上市申请人必须直接持有运营公司的最大许可权益,即境内企业主营业务如不涉及外商投资禁止/限制领域,则应搭建股权控制类的红筹架构,由境外控股公司直接持股,而不应搭建协议控制类的红筹架构。

二、搭建红筹架构的惯常步骤

无论是股权控制模式还是 VIE 模式,均需要首先进行初始离岸架构的搭建,即全体创始人在其选择的海外离岸公司注册地(如前文所述,多数红筹架构选择英属开曼群岛)共同出资设立特殊目的公司(Special Purpose Vehicle,即“SPV”)作为境外融资平台并根据商业需求逐层设立境外持股主体,同时,中国境内居民身份的创始人及其他拟持有境外融资平台权益的中国境内居民(统称“境内自然人股东”)应办理 37 号文登记。

惯常情况下,初始离岸架构的搭建主要包括如下步骤:

第一步:各境内自然人股东在一个境内公司(多数是境内的实际业务运营实体)持有股权,该境内公司将来作为 37 号文登记的权益公司会被纳入集团公司体系内。

第二步:各境内自然人股东分别在境外设立由其全资持股的 SPV,作为其各自的境外持股平台。如前文所述,境内自然人股东多数选择在 BVI 设立 SPV。此外,如果公司需要将已在境内公司设立的员工持股平台外翻至境外或需要在境外融资平台中新设员工持股平台,通常可由创始人的境外 SPV 设立一家全资 SPV,作为境外融资平台实施员工激励计划的平台。其他情况下,通常可在境外融资平台层面预留一定数量的股份或由创始人 SPV 在境外融资平台层面代持一定数量的股份(即无需设立 SPV 作为员工持股平台),作为境外融资平台实施员工激励计划的股份来源。

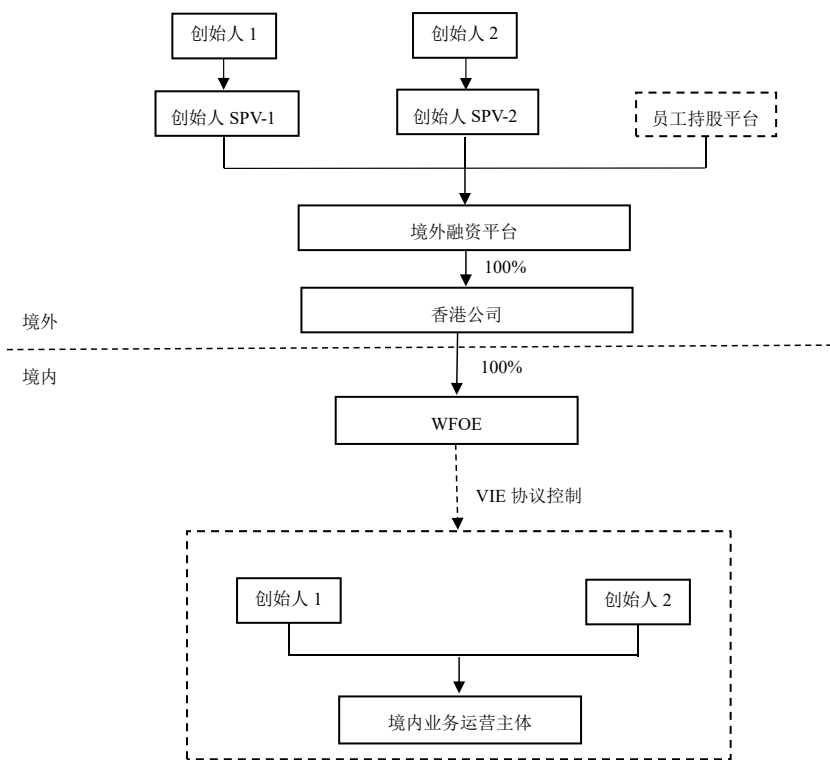
第三步:上述各境内自然人股东的境外 SPV 及作为员工持股平台的境外 SPV(如有)共同出资设立一家境外 SPV,作为境外融资平台,并办理该境外融资平台的银行开户手续。如前文所述,多数红筹架构选择在英属开曼群岛设立 SPV 作为境外融资平台。

第四步:根据《国家外汇管理局关于境内居民通过特殊目的公司境外投融资及返程投资外汇管理有关问题的通知》(汇发[2014]37 号文)(“37 号文”)的规定,境内居民以境内合法资产或权益,向注册地外汇局或者境内企业资产或权益所在地外汇局(目前权限已下放到银行)申请办理登记(俗称为“37 号文登记”)。

第五步:境外融资平台在香港设立一家全资子公司,并办理该香港公司的银行开户手续。如果项目中存在后续可能需要转让香港公司股权的商业需求,则可在境外融资平台和香港公司之间加入一层 SPV,未来可通过转让该 SPV 股份的方式间接转让香港公司股权,从而避免直接转让香港公司股权所产生的印花税。

上述步骤完成后,由“创始人 SPV(通常为 BVI 公司)—境外融资平台(通常为开曼 SPV)—香港公司”组成的初始离岸架构即准备就绪。在股权控制模式和 VIE 模式项下,离岸架构与境内架构的连接方式将存在较大区别:

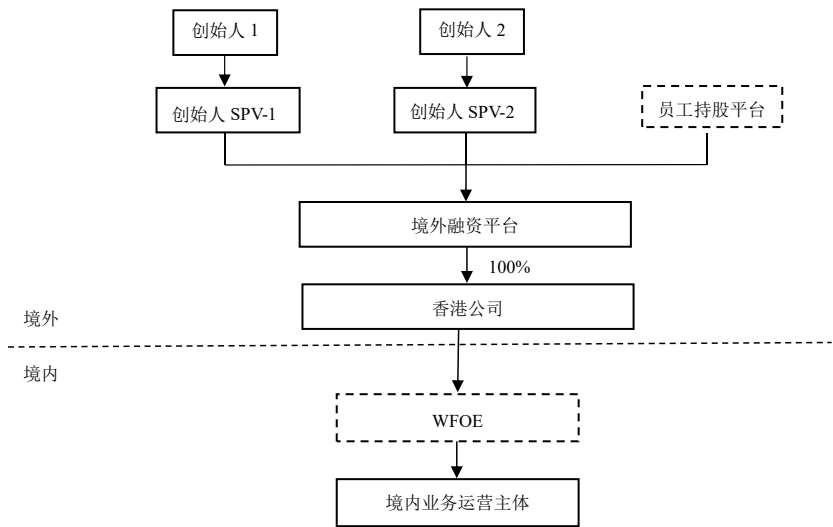
(1)VIE 模式下,在完成上述初始离岸架构的搭建且拟持有境外融资平台权益的各境内自然人股东均办理完毕 37 号文登记后,香港公司即可同步在中国境内投资新设 WFOE,由 WFOE 和境内公司以及境内公司的各股东签署一系列协议(俗称“VIE 协议”),以实现离岸架构与境内架构的连接以及境外融资平台对境内公司的间接实际控制。VIE 架构搭建完成后的图示如下:



(2) 股权控制模式下,在完成上述初始离岸架构的搭建且拟持有境外融资平台权益的各境内自然人股东均办理完毕37号文登记后,香港公司即可直接在中国境内投资新设全资子公司(即“WFOE”)作为其实际运营主体,或由香港公司或其新设的WFOE收购已有境内公司的全部股权或资产,以实现境外融资平台对境内实际运营主体的股权或资产的实际控制。

为解决《关于外国投资者并购境内企业的规定(2009年修订)》[商务部令[2009]第6号](俗称为“10号文”)下的“关联并购”的问题,实操中通常采取“两步走”的方式,即,通过引入“境外无关联第三方”将已有境内公司从纯内资公司变更为外商投资企业(Joint Venture,即“JV”)后,再由香港公司或其新设的WFOE收购JV的全部股权。

股权控制模式搭建完成后的图示如下:





跨境 劳动法遵从

第三章

第一篇 企业跨境用工安排:模式、法律风险及应对

一、跨境用工安排的现有模式

出海企业往往会根据用工需求、项目性质、运营方式等方面的不同而选择不同的用工方式,用工方式的合理选择对于用工中的法律风险防范与合规控制具有重要作用。结合司法实践及部分出海企业采用的用工安排,我们对当下跨境用工模式总结如下:

1.境外直招(Direct Recruitment Overseas)

境外直招模式是指出海企业在海外设立分支机构或子公司,直接在当地招聘员工。这种方式下,企业需要遵守当地的劳动法规定,包括劳动合同、工资、工时、福利和解雇程序等。境外直招模式的优点在于便于管理和控制,有利于本地市场的深入理解和客户关系的建立。其缺点主要在于管理成本和法律遵从成本较高。

2.外包(Outsourcing)

外包模式类同于我国的劳务分包或劳务外包,是指出海企业将某些业务或职能外包给海外服务提供商,由后者提供所需的服务或产品。外包内容可以是制造业的生产环节,也可以是IT服务、客户服务等。外包模式的主要优点在于能够有效降低成本,提高灵活性,能够极大减少法律和税务风险。显而易见,外包模式的缺点主要在于可能失去对某些核心业务控制,而且服务质量非常依赖外包服务商的质量和可靠性。

3.劳务派遣(Labor Dispatching)

劳务派遣模式主要指出海企业通过劳务派遣公司向海外派遣员工,这些员工在海外工作一段时间后返回原籍国。派遣员工通常与派遣公司签订合同,而不是与使用其劳动力的企业签订合同。劳务派遣模式的优点在于灵活性高,可以根据项目需求快速调整人员。劳务派遣模式的缺点是可能面临劳动法遵从问题,派遣员工的权益保护可能较为复杂。

4.独立承包商(Independent Contractors)

独立承包商模式主要指出海企业与海外个人或公司签订合同,以完成特定的工作或项目。独立承包商不是企业的员工,他们享有更大的自主权和灵活性,能够根据自己的专业能力和时间安排来承接项目,通常负责自己的税务和社会保障。独立承包商模式的优点在于:首先,它允许企业根据项目的具体需求快速匹配到最适合的专业人才,无需长期雇佣和维持庞大的员工队伍。其次,独立承包商通常具有高度的专业技能和经验,能够确保项目的高质量完成。再者,由于独立承包商自负盈亏,出海企业无需承担其社保、福利等额外成本,有助于控制运营成本。独立承包商模式的缺点:需要确保承包商的真实独立地位。此外,由于独立承包商并非企业的正式员工,企业难以直接控制其工作流程、质量和进度。这种不确定性可能导致项目延期、成本超支或质量不达标的风险增加。

5.远程工作(Remote Work)

远程工作模式是几乎所有的出海企业都在采用的混合用工模式中的一种工作模式,主要指出海企业利用互联网技术,允许员工在海外远程工作。这种用工方式适用于知识型工作,如编程、设计、写作等。远程工作模式的优点在于降低办公成本,提高员工满意度,扩大人才库,同时对于部分核心技术、专利等能够起到很好地保护作用。远程工作模式的缺点主要是可能存在时差、沟通和管理挑战。

6.合资企业(Joint Ventures)

合资企业模式是人力与资本结合的最典型方式之一,合资企业模式的主要内容为企业与海外当地企业共同投资设立新的企业,共同运营和管理。用工方式可以是直接雇佣,也可以是其他方式。合资企业模式的优点是可以利用当地企业的资源 and 市场知识,分担风险。合资企业模式的缺点在于可能存在合作伙伴间的管理和文化冲突。

7.特许经营(Franchising)

特许经营模式是指企业授权海外企业在特定区域内使用其品牌、商业模式和技术进行运营,特许经营方通常负责当地的用工和管理。这种模式实际上并不完全属于一种用工模式,但是由于该模式对企业用工方式的采用具有直接影响作用,且在实践中(尤其指东南亚地区)运用较为普遍,本文对此予以列明。

特许经营模式的优点在于能够快速扩张市场,减少直接投资和运营风险。特许经营模式的缺点在于对特许经营方的控制和监督可能较为有限。

二、跨境用工安排涉及的法律风险

贯穿于用工招聘至雇佣关系解除及其后的后合同义务履行全过程。本文主要对雇佣合同的签订、雇佣合同的履行及发生法律纠纷处理中的用工风险予以分析,旨在帮助出海企业明确各个阶段所面临的具体法律风险。

(一)合同签订阶段

雇佣合同或者准确说“劳动合同”的签订是用工风险源所在,我们梳理了近5年发生的典型跨境用工案例,总结了劳动合同签订中主要的九大风险点:

1.劳动法遵从风险

在全球化的浪潮下,出海企业面临着前所未有的挑战,其中之一便是劳动法遵从风险。不同国家和地区的劳动法规定犹如万花筒般绚烂多彩,却又各自为政,差异显著。以工时制度为例,有的国家实行严格的八小时工作制,而有的地区则允许更灵活的工作时间安排。再如休假政策,各国的年假、病假、产假等规定千差万别,出海企业稍有不慎便可能触犯法律红线。因此,出海企业在进入新市场前,务必深入研究当地的劳动法规定,确保劳动合同的每一条款都符合当地法律要求,否则,合同可能被视为无效,企业将面临罚款、诉讼等严重后果。

2.合同条款不明确

劳动合同作为企业与员工之间的法律纽带,其条款的明确性至关重要。然而,在实际操

作中,不少出海企业的劳动合同往往存在表述不清的问题。比如,对于工作职责的描述模糊不清,导致员工与企业在工作内容上产生分歧;薪酬条款含糊其词,使得员工对于自己的收入状况感到困惑;工作地点、合同期限等关键信息也未能明确界定,为企业后续管理埋下隐患。因此,企业在制定劳动合同时,务必做到条款清晰、明确,以减少不必要的法律风险。

3.雇佣类型错误

在签订劳动合同时,出海企业还需谨慎区分雇佣类型。错将员工分类为独立承包商而非正式员工,看似可以节省成本,实则可能给企业带来更大的麻烦。因为独立承包商与正式员工在法律地位、税务处理等方面存在显著差异。一旦企业错误地将员工归类为独立承包商,便可能面临税务罚款、补缴税款和员工索赔的风险。此外,各国、各地区对于雇佣关系的认定标准也不尽相同,出海企业在制定雇佣策略时,需充分考虑当地法律法规的差异性,确保符合当地规定。

4.隐私和数据保护

在数字化时代,个人隐私和数据保护已成为全球关注的焦点。出海企业在签订劳动合同过程中,往往会收集和员工处理员工的个人信息。这些信息包括但不限于姓名、联系方式、身份证号、银行账户等敏感数据。如果企业未能妥善保管这些信息,或者未经员工同意便擅自泄露给第三方,便可能触犯当地的隐私和数据保护法律。因此,出海企业在处理员工个人信息时,务必遵守当地的法律法规要求,建立健全的数据保护机制,以保障员工的合法权益。

5.歧视和平等就业

平等就业是现代社会的核心价值观之一。然而,在实际操作中,一些出海企业的劳动合同中却可能含有歧视性内容。比如,基于性别、年龄、种族、宗教等因素的招聘和雇佣歧视便是一种典型的违法行为。这些歧视性条款不仅违反了平等就业法规,还可能损害企业的社会形象和声誉。因此,出海企业在招聘和雇佣过程中需确保公平对待所有候选人,避免任何形式的歧视行为。

6.社会保险和福利

社会保险和一般福利性待遇是跨境用工中的重要合规点。不同国家的社会保险制度差异较大,出海企业在为员工缴纳社会保险费用时需格外小心。如果企业未能按照当地规定为员工缴纳社会保险费用,便可能面临法律责任。此外,一些国家还规定了员工应享有的其他福利待遇,如带薪年假、带薪病假、生育保险等。出海企业需充分了解当地的福利政策并予以落实,以保障员工的合法权益并提升企业的竞争力。

7.税务风险

跨境用工还可能涉及双重征税问题。由于不同国家的税法规定存在差异,出海企业在为员工发放薪酬时需考虑税务处理的问题。如果企业未能正确履行税务申报和缴纳义务,便可能面临税务审计和罚款的风险。因此,出海企业在制定劳动合同和薪酬政策时,需明确税务责任并咨询专业税务顾问的意见以确保合规性。

8.移民和签证问题

跨境用工还可能涉及工作签证和居留许可的问题。出海企业需确保员工持有合法的工作签证和居留许可以便在目标国家合法工作。如果企业未能为员工提供必要的签证支持或

未能及时办理签证续签手续便可能导致员工无法合法工作并给企业带来法律风险。因此出海企业在跨境用工前需充分了解当地的移民政策并提前为员工办理好相关手续以避免不必要的损失。

9. 合同终止及解除条款

合同终止及解除条款是劳动合同中的重要组成部分。这些条款的合理性和合法性直接关系到企业与员工之间的权益平衡。如果合同终止及解除条款不合理或不符合当地法律便可能在解雇员工时引发争议并导致企业面临高额的赔偿金。因此,出海企业在制定合同终止及解除条款时需充分考虑当地法律法规的要求并咨询专业法律顾问的意见以确保条款的合法性和合理性。同时企业还需注意在解雇员工时应遵守当地的解雇程序和规定,以避免因程序不当而引发的法律风险。

(二) 合同履行阶段

劳动合同能否全面且因地制宜地履行,对是否引发用工法律风险具有决定性作用。经梳理,我们认为劳动合同履行阶段主要法律风险如下:

1. 劳动法遵从风险

在全球化经营的大背景下,出海企业不仅要应对市场的波动,还需密切关注并遵守各国的劳动法规定。这些规定通常涵盖工时管理、加班制度、休假安排以及薪酬支付等多个方面。例如,在某些国家,超时加班被视为违法行为,而另一些国家则对加班费有明确的计算标准。若出海企业未能准确理解和执行这些规定,不仅可能面临高额的罚款,还可能引发员工的集体诉讼,对企业的声誉和财务状况造成严重影响。

在具体实践中,出海企业需通过详细的研究和咨询,确保其政策和实践与当地法律保持一致。例如,可以通过聘请当地法律顾问、定期进行内部培训以及建立合规审查机制等方式,来降低劳动法遵从风险。此外,企业还应积极响应员工关切,建立有效的沟通渠道,以便及时发现并解决问题。

2. 工作条件和环境

为员工提供一个安全、健康的工作环境,是出海企业不可推卸的责任。这不仅关系到员工的身体健康和生命安全,也是企业履行社会责任的重要体现。如果出海企业未能提供符合当地法律标准的工作条件和环境,如缺乏必要的防护设备、未定期进行安全检查等,将面临健康和安全方面的违规风险。这不仅可能引发监管部门的处罚,还可能导致员工受伤或患病,进而引发赔偿责任和声誉损失。

为了降低这一风险,出海企业需加强工作场所的安全管理,确保所有设备符合安全标准,并定期维护和检查。同时,企业还应建立完善的应急预案和救援机制,以便在发生紧急情况时能够迅速应对。

3. 薪酬和福利

薪酬和福利是员工最为关心的问题之一。出海企业在制定薪酬和福利政策时,需充分考虑当地法律法规的要求以及员工的实际需求。如果企业错误计算或延迟支付工资、奖金、津贴等福利,或未能按照法律规定为员工缴纳社会保险、医疗保险等费用,将违反境内外劳动法

规定,还可能引发员工的投诉和索赔。

为了避免这一风险,出海企业需建立完善的薪酬和福利管理制度,确保所有支付和缴纳都符合当地法律法规的要求。同时,企业还应加强与员工的沟通,及时了解员工的反馈和需求,以便对政策进行必要的调整和优化。

4.员工解雇和裁员

在解雇或裁员过程中,出海企业需严格遵守当地的程序和法律要求。如果企业未能履行必要的通知、协商或补偿等程序,将构成不当解雇,进而引发法律诉讼和赔偿。这不仅会增加企业的法律成本,还可能损害企业的声誉和形象。

为了降低这一风险,出海企业需提前制定详细的解雇或裁员计划,并确保所有程序都符合当地法律法规的要求。同时,企业还应积极与员工进行沟通和协商,尽可能减少员工的损失和不满情绪。

5.数据保护和隐私

在劳动合同履行过程中,出海企业通常需要处理员工的个人信息。如果企业未能遵守当地的数据保护法律,如未经员工同意擅自收集、使用或泄露其个人信息,将面临法律责任和罚款。

为了保护员工的个人信息安全和隐私权益,出海企业需建立完善的数据保护管理制度和技术措施。例如,可以通过加强数据加密、访问控制和审计追踪等方式来确保数据的安全性和完整性。同时,企业还应加强员工的培训和教育,提高员工的数据保护意识和能力。

6.员工健康和安

员工健康和安是全球范围内ESG人力资源合规评价体系中的重要组成部分。出海企业需高度重视员工的健康和安问题,加强工作场所的安全管理和健康监测工作。如果企业在劳动环境安全方面存在疏忽,未能确保劳动环境的安全性或未能及时发现并妥善处理健康隐患等,将导致员工面临受伤或患病等重大风险,进而引发企业的赔偿责任和声誉损失等多重风险。

例如江苏省南通市海门区法院审理的一起劳动纠纷,就是由于出海企业未能为员工提供安全的劳动环境而导致员工受伤并引发诉讼。这一案例不仅提醒出海企业要高度重视员工的健康和安问题,还强调了加强工作场所安全管理和健康监测工作的重要性。

7.合同变更

劳动合同是保障员工和企业双方权益的重要法律文件。在合同履行过程中,如需修订、变更或解除合同条款,需遵循当地法律法规的规定并履行必要的程序和要求。企业如果未经员工同意或不符合法定程序擅自变更劳动合同条款,可能构成违法行为,引发争议和诉讼等风险。

为了降低这一风险并维护员工的合法权益和企业的声誉形象等核心利益,企业在签订、变更或解除劳动合同时需要充分尊重员工的意愿和利益诉求,并加强沟通协商的力度,确保双方能够达成共识,妥善处理相关问题。此外,企业还需要加强内部管理和制度建设,确保合规经营,从而降低法律风险的发生概率。

8.税务和社保合规

税务和社保是出海企业必须面对的重要问题之一。如果企业未能正确申报和缴纳员工

的个人所得税、社会保险和其他相关税费,将面临税务审计和罚款等风险,这些问题一旦出现,将严重威胁企业的财务健康。同时这种不合规行为还会影响企业的信誉度和声誉,增加利益受损的可能性,影响企业的长期发展。因此出海企业需要加强税务和社保合规管理工作,建立健全相关制度和技术手段,确保合规经营,从而有效控制和降低各类风险问题的发生概率。

9.移民和居留问题

对于涉及跨国经营或海外投资的出海企业来说,还需要关注移民和居留等相关问题,因为这些问题出现的往往较高。一旦员工的工作签证或居留许可过期或不符合当地规定,出海企业可能面临非法用工等法律风险,这不仅是会影响企业的正常运营,还可能引发一系列连锁反应,如员工权益受损、政府处罚、社会舆论压力等。因此出海企业需要加强移民和居留管理工作力度,与当地政府部门建立和保持密切沟通和协作关系,确保员工能够合法居留,从而有效控制并降低法律风险问题的发生概率,保障企业的稳健发展。

10.劳动争议

在劳动合同履行过程中,可能会因各种原因触发劳动争议,进而增加法律诉讼等风险的发生概率。为了降低这一风险并维护员工和企业双方的权益,加强沟通协商和调解等工作显得尤为重要。通过加大这些工作的力度,可以更有效地处理相关争议,寻求双方都能接受的解决方案,从而确保问题得到有效解决。与此同时,企业还需强化内部管理和制度建设,以提升应对劳动争议等问题的能力,进一步降低风险的发生概率,确保问题得到有效控制和解决。至于劳动合同不恰当履行所引发的具体劳动争议风险点,本文将在下一章节中进行详细分析。

(三)争议解决阶段

跨境用工在劳动争议解决阶段可能面临的法律风险较为复杂,经检索近五年的较为典型的跨境用工劳动争议案例,我们总结劳动争议解决阶段的法律风险主要有以下九点:

1.法律体系的多样性与冲突

跨境用工之所以复杂,首先在于不同国家的法律体系之间存在显著的差异。这些差异不仅体现在法律条文上,更深入到法律解释、司法实践乃至文化背景之中。例如,美国法律体系强调判例法的重要性,而欧洲大陆国家则更多地依赖成文法。这种差异使得企业在面对争议时,需要仔细分析各国的法律规定,以确定最适合的法律适用原则。然而,这种分析往往耗时费力,且结果充满不确定性。

此外,不同国家之间的法律冲突也加剧了法律适用的不确定性。例如,当劳动合同中的某些条款与某国法律相抵触时,这些条款是否有效、如何解释以及如何执行等问题都可能引发争议。这种争议不仅增加了法律成本,还可能导致企业陷入长时间的诉讼泥潭。

2.管辖权问题

在跨境用工争议中,管辖权的确定同样是一个棘手的问题。由于跨境用工涉及多个国家的法律,很难确定哪个国家的法院或仲裁机构具有管辖权。这种不确定性不仅让企业难以选择合适的争议解决途径,还可能使企业面临在多个国家被起诉的风险。一旦出现这种情况,

企业不仅需要应对复杂的法律程序,还需要承担高昂的法律费用和时间成本。

3.证据收集的难题

在跨境争议中,证据的收集和呈递也是一大挑战。由于不同国家的法律对证据的要求和认可标准存在差异,因此企业很难确保所收集的证据在所有相关国家都具备合法性和可接受性。此外,语言、文化和法律障碍也可能阻碍证据的收集和呈递工作。例如,在某些国家,某些类型的证据可能被视为非法或不可接受;而在另一些国家,这些证据则可能被视为关键证据。这种差异使得企业在跨境争议中很难取得有利的证据支持。

4.法律程序与时效的考验

不同国家的法律程序和时效规则也可能给跨境用工带来挑战。企业如果未能及时响应或遵循正确的程序,可能会丧失辩护(或答辩)权利。例如,在某些国家,企业必须在规定的时间内提交答辩状或提供证据;而在另一些国家,则可能允许更长的准备时间。这种差异使得企业在面对跨境争议时必须格外谨慎,以免因疏忽而错失辩护机会。

5.赔偿标准的差异与赔偿风险

各国对于赔偿标准的规定也存在显著差异。这种差异不仅体现在赔偿金额上,还可能涉及赔偿范围、计算方式等方面。因此,出海企业在跨境用工中可能面临高额的赔偿风险。更为严重的是,企业还可能面临支付双重赔偿的风险。例如,在员工母国和工作国都面临索赔的情况下,企业需要同时满足两个国家的赔偿要求。这种双重赔偿的风险不仅增加了企业的经济负担,还可能对企业的声誉和形象造成负面影响。

6.和解与调解的限制

在某些国家,和解和调解可能受到法律限制或执行困难。这种局限使得企业在跨境争议中难以通过和解或调解方式快速解决争议。即使双方达成了和解协议,也可能因执行困难而无法得到有效履行。这种情况不仅增加了企业的法律成本和时间成本,还可能使争议进一步升级和恶化。

7.仲裁裁决的承认与执行

仲裁作为一种重要的争议解决方式,在跨境用工中同样面临着承认与执行的难题。以竞业限制(含企业用工的不正当竞争)为例,即使企业在仲裁中获胜并获得了有利的裁决结果,也可能面临仲裁裁决在外国法院不被承认或难以执行的风险。这种风险不仅使企业的仲裁努力付诸东流,还可能使企业面临更大的法律风险和经济损失。

8.公共关系与声誉风险

跨境劳动争议还可能引起媒体关注和社会舆论的广泛讨论。这种关注不仅可能对企业的国际形象和声誉造成负面影响,还可能引发消费者信任危机和市场份额下降等连锁反应。因此,企业在处理跨境劳动争议时必须格外谨慎和敏感,以免因处理不当而引发更大的公共关系危机和声誉风险。

9.后续雇佣关系的挑战

争议解决后,出海企业还需要与员工维持或重新建立雇佣关系。这种关系的修复和重建不仅涉及法律层面的问题(如合同的重新签订、权益的重新分配等),还涉及信任和合作的问题。在争议解决过程中,双方可能产生一定的隔阂和不信任感;因此,在争议解决后如何重建

信任和合作关系成为企业面临的一大挑战。

综上所述,跨境用工的法律适用不确定性是一个复杂而严峻的问题。为了应对这一挑战并降低法律风险,企业需要充分了解各国的法律规定和司法实践;在选择争议解决途径时谨慎考虑并选择合适的方案;在收集证据和准备辩护时充分准备并遵循正确的程序;在赔偿和解方面积极寻求合理的解决方案;在仲裁裁决的承认与执行方面积极争取并维护自身权益;在公共关系和声誉管理方面加强沟通和宣传以树立良好的企业形象;在后续雇佣关系方面努力修复和重建信任和合作关系以实现共赢发展。另一方面,从法律的指引、评价作用来看,确实存在诸多案例显示,在其他跨境用工中,当劳动者发现同类型用工纠纷中的其他劳动者获得高额的赔偿或补偿后,往往会效仿这些成功案例,通过仲裁、诉讼等法律途径来维护自身权益。这种行为给出海企业的用工管理带来了极大的困扰和挑战。

三、跨境用工的合规建议

(一)跨境用工中的劳动关系建立合规

跨境用工中的劳动关系建立合规是一个复杂的过程,涉及不同国家的法律、文化和社会实践。根据前文所述的跨境用工中的主要法律风险,我们总结跨境用工的合规体系建设应当主要从以下十一点出发:

1.了解当地法律法规

企业应深入研究并了解目标国家的劳动法律法规,包括雇佣合同、工作时间、休假制度、薪酬福利、劳动保护、解雇程序等方面的具体规定。这不仅有助于避免违法用工的风险,还能确保企业的运营符合当地的法律要求,维护企业的合法权益。

2.确定雇佣关系

根据当地法律明确员工的雇佣类型,如全职、兼职、固定期限合同、独立承包商等。确保雇佣关系的分类符合实际情况,避免误分类带来的法律风险。

3.劳动合同的制定与签署

制定符合当地法律要求的劳动合同模板,包括合同条款、工作职责、薪酬、福利、合同期限等。确保劳动合同以当地官方语言书写,并提供翻译版本以便员工理解。劳动合同应由双方签署,并保留书面记录。

4.工作许可和签证

了解目标国家的工作签证、用工许可的申请流程、要求和续签规定。为外籍员工办理合法的工作许可和签证,确保其有权在目标国家工作。

5.社会保险和福利

根据当地法律规定为员工缴纳社会保险,如养老保险、医疗保险、失业保险等。提供符合当地标准的福利待遇,如带薪休假、病假、产假等。

6.薪酬支付

确定员工的薪酬结构,包括基本工资、奖金、津贴等。遵守当地的薪酬支付规定,包括支

付周期、方式、税前税后等。

7.个人所得税和税务合规

了解并遵守当地的个人所得税扣缴规定。确保企业的税务登记和申报符合当地税法要求。

8.员工档案管理

建立和维护员工档案,包括个人资料、合同、薪酬记录、考勤等。确保档案管理的安全性,防止数据泄露。

9.劳动保护和健康安全

提供符合当地标准的劳动保护措施和健康安全的工作环境。定期进行健康和安全培训,预防职业疾病和事故。

10.员工培训与沟通

为员工提供必要的入职培训和定期的技能提升培训。建立有效的沟通机制,确保员工了解其权利和义务。

11.合规监控与审计

定期对劳动关系的合规性进行内部审计和评估。及时纠正发现的不合规问题,并采取措施预防未来的违规行为。

(二)跨境用工中的培训与绩效考核

在以人工智能、数据、互联网集群出海时代,出海员工的素质,特别是企业管理人员的素质是出海企业在国际竞争中获胜的重要因素。职工培训是提升出海员工素质必然途径之一。中国企业或中资企业在出海过程中,其使用的绩效管理往往沿用本国考核标准而未考虑绩效考核在文化等方面的特殊性。对国际人力资源考核的特殊性认识不到位使得中国企业在国际化经营与管理过程中存在着一定的人力资源考核风险。

1.跨境用工中的培训

对于出海企业而言,常规的职工培训很难满足人员素质提升及劳工输出地文化等方面的要求。这种情况下,具有针对性的跨境劳工培训就显得尤为重要。

在与诸多出海企业沟通中发现,大多数出海企业都片面地认为跨境人力资源培训的主要内容就是对文化的认识,比如敏感性训练、语言学习、跨文化沟通及冲突处理、地区环境模拟等。然而,跨境人力资源培训的内容除了跨文化培训外,当然还必须进行各方面实际业务的培训,比如管理培训、技术培训、制度培训、操作规程培训等。

我们认为跨境劳动培训应以以下五点为抓手:

(1)重视文化培训。有效的文化培训有助于出海企业的劳动者适应新的跨文化背景下的生活和工作环境,更有利于业务的交涉与产品融合。培训主要包括区域文化界别、宗教文化界别、种族文化界别;(2)培训出海企业的劳动者的文化敏感性。在文化领域内发生的“说者无心,听者有意”而引发冲突的案例比比皆是,大多是因为出海企业的劳动者的文化敏感性不够。培训有两个主要内容:一是系统培训有关母国文化背景、文化内涵和区别于其他文化的主要特点;二是培训外派管理人员对东道国文化特征的理性和感性分析能力,掌握东道国文

化的主干精髓;(3)坚持系统性、持续性的文化培训;(4)改变出海企业的劳动者培训的传统观念。跨境劳动培训不仅旨在提升劳工的工作技能,更为加强劳工的工作安全与职业安全;(5)形成系统化的出海劳工培训机制。一方面,将劳工培训、选用、选拔等统一归由企业人资部门管理。另一方面改变传统的“听课”方式,通过前期课堂学习、后期项目参与等方式进行综合性培训。

2.跨境用工中的绩效考核

由于出海企业或出海项目的绩效考核方案不健全、项目运营的多变、东道国政策的更迭等,使得以市场占有率、利润率、投资收益率等财务指标为主要内容的绩效考核标准难以准确达到出海企业制定的绩效目标。

跨境用工中的绩效考核目标包括战略方向和业绩。在绩效考核中突出战略方向,有利于实现企业的长远发展。例如员工在财务、客户关系、员工关系和合作伙伴之间的一些作为,也包括员工的领导能力、战略计划、客户关注程度、信息和分析能力、人力资源开发、过程管理等方面的表现,要求较为全面、合理、综合地反映一个员工的各方面的业绩。

出海企业的劳动者越来越趋向知识型,这些员工不仅在追求高薪酬,同时也在追求自我价值的实现。员工对于公平感、自我实现、工作本身对人的激励等在工作中的体现要求越来越多,因而对于管理者的素质要求越来越高。如何选拔优秀的管理者,如何明确定义管理者的素质,同时如何培训管理者,都显得越来越重要。

(三)跨境用工中的薪酬合规

《劳动法》《劳动合同法》及《工资支付暂行规定》等法律法规规定了劳动者通过劳动获得劳动报酬的权利,工资应当以货币形式按月支付给劳动者本人,用人单位不得克扣或者无故拖欠劳动者的工资。

实践中,多数企业将员工派至境外工作前会要求员工与境外企业签订劳动合同,由境外企业与外派员工建立劳动用工关系。在工资支付中,往往采取“单一支付”以及“境外境内企业分别支付”方式。



1.全部由境外企业支付

境外企业向外派员工支付劳动报酬基于双方就外派事宜签订的劳动合同的约定。除工资支付外,此种劳动合同还会明确考核要求、用工管理、休息休假、法律适用及争议解决方式。在外派员工与境外企业建立劳动关系,且境内外企业不存在混同用工的情形下,外派员工要求中国境内企业支付其外派期间工资的诉求较难得到支持。

确定管辖权是我国法院审理涉外劳动用工争议案件的首要步骤。法院在适用《涉外民事关系法律适用法》第四十三条^[1]确定涉外劳动用工争议案件管辖权时作出了“利于劳动者的适度偏离”,即便与中国境外企业签订劳动合同,如劳动者与中国境内企业符合劳动关系中人身、经济和组织从属性特征,则法院也可能会认定劳动者与中国境内企业存在事实劳动关系,从而认定争议案件属于我国法院管辖范围。但是,如劳动者工作地点位于境外,与境外用人单位签订劳动合同,工资由境外企业全额发放且受境外用人单位劳动管理,则不属于我国法院管辖范围。处理此类劳动争议案件时,一审法院常常会在实质审理后,裁定驳回起诉。

以董某会与中国某冶金公司劳动争议案^[2]、柳某双与中国某冶金公司劳动争议案^[3]劳动争议案的一审、二审与再审为例,法院均认为外派员工诉请的各项争议所涉事实均系其于中国境外与境外公司劳动关系存续期间产生,属于涉外劳动争议,应适用我国有关涉外民事诉讼的特别规定,排除了中国法院实体管辖。

2.境外境内企业分别支付

境外境内企业分别支付工资的模式多见于中国境内外企业之间的约定,通常将外派员工基本工资、外派补贴、绩效奖金等分为多个部分,由境内外企业分别发放。在出现有关劳动报酬纠纷时,境内企业多以其“已按照约定履行完毕境内工资发放义务,非境外工资的发放主体”为由拒绝支付外派员工的境外工资、补贴或其他劳动报酬。但在司法实践中,即便中国境内外企业间存在协议约定,如果两个企业属于关联企业或法院认定劳动者与境内企业劳动关系存续或存在事实劳动关系,则中国境内企业仍需就境外企业未支付的工资、补贴差额承担支付责任。

在宁夏某锰业公司与雍某劳动争议案中,雍某在宁夏某锰业公司工作期间被外派至该公司下属联合矿业公司加纳锰业有限公司,工资分为国内与国外两部分,由两公司按月分别核算后发放。针对海外未付工资部分,宁夏某锰业公司主张雍某在加纳外派期间工资由海外公司支付,海外公司作为发放主体,有权决定发放金额以及是否发放,未付部分不应由宁夏某锰业公司承担。法院认为,雍某在劳动关系存续期间由宁夏某锰业公司外派至加纳工作,该公司负有用人单位及时足额支付工资的法定义务,宁夏某锰业公司应向雍某支付加纳锰业有限公司未足额支付部分的工资。^[4]

综合上述案例,仅从避免劳动争议的角度,中国对外投资企业在向外派员工发放工资时适用单一工资发放模式,潜在风险相对最低。

[1]《涉外民事关系法律适用法》第四十三条规定:“劳动合同,适用劳动者工作地法律;难以确定劳动者工作地的,适用用人单位主营业地法律。劳务派遣,可以适用劳务派出地法律。”

[2]参见(2015)阳民初字第2183号民事判决书。

[3]参见(2018)鄂0203民初100号民事判决书。

[4]参见(2022)宁05民终122号民事判决书。

但是,与民法法域下交易主体的公平买卖、意思自治有所不同,劳动法法域同时更为强调社会公平和对弱势群体(劳动者)的倾斜保护。有观点认为,为外派员工按时足额支付工资是中国对外投资企业的义务。因此,不论中国对外投资企业面临何种经营困难,都应按时、足额发放劳动报酬,不得以不可抗力为由进行抗辩。例如,在北京某软件公司与王某劳动争议案中,北京某软件公司以中美贸易危机和新冠疫情加剧经营困难为由称其延迟支付王某奖金、补贴等具有合理性的抗辩,未能得到法院的支持。此外,因北京某软件公司拖欠劳动报酬,王某还有权依法获得解除劳动合同经济补偿金。^[5]

(四)跨境用工中的社会保障合规

缴纳社会保险是法律规定的用人单位的强制性责任。若外派员工与派遣目的地的当地企业签订了劳动合同并建立了劳动关系,那么当地企业必须根据其所在国家的法律规定,为外派员工办理社会保险的注册和缴纳。通常情况下,外派员工与境外企业之间因社会保险的缴纳和待遇领取等问题产生的争议,将由当地法院或政府部门负责解决。然而,如果外派员工是在境内企业的安排下被派往境外工作,或者被法院判定与境内企业存在劳动关系,那么境内企业将面临同时缴纳境内和境外社会保险的双重责任。

1.社会保险缴纳

在实际操作中,许多从事对外投资的企业为了减少劳动力成本,选择在派遣员工到国外工作后停止为其缴纳国内的社会保险。这种做法潜在地引发了双方的矛盾和劳动争议,不利于保护外派员工的劳动权益。尽管在我国,社会保险的征收是社保经办机构(目前由税务部门代为征收)的职责,但在审理与社保缴纳相关的争议时,法院通常以不属于其受理范围为由,不支持外派员工的相关诉求。

例如,在宁夏某锰业公司与雍某劳动争议案中,二审法院撤销了一审判决中“要求宁夏某锰业公司为雍某缴纳社会保险”的判项,认为一审法院直接判决宁夏某锰业公司为雍某缴纳社会保险超出了人民法院裁判范围,应予纠正。^[6]与该案持相同观点的还有游某舟与莆田市某投资公司劳动争议案、徐某姝与福建某镍业公司劳动争议案以及殷某与北京某国际商务服务公司劳动争议案。

但是,外派员工仍可以向社保稽核部门投诉与举报,一旦被认定存在漏缴或断缴社会保险,除依法补缴外,对外投资企业还面临着高额的滞纳金处罚。

2.损失赔偿

社会保险的缴纳属于行政法律关系,但如因对外投资企业漏缴或断缴社会保险造成外派员工利益损失的,对外投资企业应就损失数额向外派员工承担赔偿责任。例如,在某建设公司与梁某等劳动争议案中,因某建设公司未如实足额按照工资发放标准为宣某某(梁某直系亲属)缴纳工伤保险,导致其直系亲属无法足额领取供养亲属抚恤金,最终该公司被判决向梁某等补足差额。^[7]与该案情况相似的还有湖南某桥隧建筑公司与程某劳动争议案,法院认为

[5]参见(2023)京02民终10100号民事判决书。

[6]参见(2022)宁05民终122号民事判决书。

[7]参见(2022)京01民终5675号民事判决书。

因湖南某桥隧建筑公司未依法为程某在国内参加失业保险,导致程某无法享有失业保险待遇,故该部分损失应由湖南某桥隧建筑公司承担。但需要强调的是,外派员工主张因对外投资企业未缴纳或少缴社会保险对其造成损失的,应承担举证责任。在本案中,因程某因未提供自行补缴养老保险金的证据,亦未出现因社会保险经办机构不能补办导致其无法享受养老保险待遇的情形。所以,法院未支持程某要求湖南某桥隧建筑公司赔偿养老保险待遇损失的请求。^[8]

3.补充保险

为有效规避意外风险并减轻用工主体责任,购买意外保险和进行损失赔偿是至关重要的。除了缴纳工伤保险,许多对外投资企业还会在与外派员工签订的劳动合同中约定为员工购买人身意外保险。这样一来,一旦发生意外,保险公司将对员工本人或其近亲属进行赔偿。然而,人身意外险的赔付金额并不能用来抵扣工伤保险待遇。即便对外投资企业未依法缴纳工伤保险,外派员工在获得人身意外险赔付后,依然有权要求企业承担工伤保险待遇。

此外,有观点指出,尽管购买意外保险并非中国对外投资企业的法定责任,但如果企业对外派员工承诺购买保险却未能履行,导致外派员工或其近亲属遭受损失,企业则可能需要承担违约或赔偿责任。

除了人身意外险,对外投资企业通常还会购买雇主责任险。需要注意的是,雇主责任险并不能替代人身意外险,且可能带来额外的企业责任风险。进一步而言,二者主要区别在于保险对象不同,人身意外险保险对象为外派员工,而雇主责任险保险对象为对外投资企业自身。在韩某辉与深圳市水湾远洋渔业有限公司福利待遇纠纷案中,韩某海与深圳市某远洋渔业公司签订的《劳动合同》约定该公司为韩某海购买意外险或者商业保险,但未对购买险种作出明确。后因深圳市某远洋渔业公司在工伤保险之外仅购置了雇主责任险,导致韩某海在莫桑比克安哥谢因突发疾病死亡后其近亲属韩某辉无法获得保险赔偿。处理争议时,法院从合同目的及通常解释出发,将所约定保险定义为“公司作为投保人、韩某海作为受益人的保险。”据此,深圳市某远洋渔业公司未按约定为韩某海购买保险的行为构成违约,应当向韩某海唯一继承人韩某辉承担相应责任。^[9]

因此,如劳动合同或外派协议等约定对外投资企业为外派员工购买意外险或商业保险,但未对具体保险作出明确约定,或应解释为“为劳动者而非为雇主利益”购买的商业保险。对外投资企业未按照劳动合同等约定购买特定险种保险,构成违约。因其违约行为造成外派员工或其近亲属损失的,可能被要求承担违约或赔偿责任。

(五)跨境用工中的税务合规

跨境用工为企业带来人力资源优势的同时,也带来了诸多税务合规问题。税务合规是企业合规管理的重要组成部分,对于维护企业合法权益、降低税收风险具有重要意义。

1.跨境用工中的税务

(1)国际税收协定适用问题

[8]参见(2019)湘09民终1432号民事判决书。

[9]参见(2021)粤民终2912号民事判决书。

跨境用工涉及不同国家(地区)的税收政策,企业在适用国际税收协定时,可能面临以下问题:A:协定选择:企业在跨境用工过程中,可能涉及多个税收协定,如何选择适用协定成为难题。B:协定解释:不同国家(地区)对同一协定的解释可能存在差异,导致企业在税务合规方面产生分歧。

(2)居民身份认定问题

跨境用工中,员工可能同时在两个或多个国家(地区)产生纳税义务。如何界定员工的居民身份,成为税务合规的关键。

(3)所得来源地认定问题

跨境用工中,员工的收入可能来自多个国家(地区)。如何准确划分所得来源地,对于税务合规具有重要意义。

2.跨境用工税务合规对策及建议

(1)建立健全税务合规管理体系

企业应建立健全税务合规管理体系,包括以下几个方面:A:制定税务合规政策:明确企业跨境用工税务合规的目标、原则和流程。B:设立税务合规部门:负责跨境用工税务合规的日常工作。C:加强税务合规培训:提高员工对跨境用工税务合规的认识和重视程度。

(2)合理选择国际税收协定

企业在跨境用工过程中,应合理选择国际税收协定,如:A:充分了解协定内容:企业应深入研究相关税收协定,了解协定条款的具体含义。B:咨询专业意见:企业可聘请专业税务顾问,为企业提供协定适用的专业意见。

(3)明确居民身份和所得来源地

企业应明确员工的居民身份和所得来源地,如:A:了解各国(地区)税法规定:企业应熟悉各国(地区)关于居民身份和所得来源地的税法规定。B:签订劳动合同:明确员工的工作地点、职责范围等,为界定居民身份和所得来源地提供依据。

跨境用工中的税务合规问题复杂多样,出海企业应高度重视,采取有效措施加以应对。通过建立健全税务合规管理体系、合理选择国际税收协定、明确居民身份和所得来源地、关注社会保险合规等方面,企业可以有效降低跨境用工中的税务风险

(六)跨境用工中的员工控制

出海企业员工(尤其指主要项目管理人员)的失控无疑会给出海项目及企业带来毁灭性打击,因此,制定一套完善的具有可行性的员工控制方案、措施对出海企业的稳定、可持续发展具有重要作用。

第一,制定清晰、具体且易于执行的项目管理政策和程序是至关重要的。这不仅包括明确的工作职责和期望,还应涵盖项目时间线、预算规划以及风险评估等方面的内容。这些政策与程序将为项目人员提供明确的指导,确保他们始终朝着项目目标努力。

第二,为了更有效地监控项目进度和人员表现,出海企业可以采用先进的项目管理工具和软件。这些工具通常具备实时数据追踪、报告生成和自动提醒等功能,使出海企业能够随时掌握项目的最新动态。同时,通过数据分析,出海企业还可以发现潜在的问题和瓶颈,并及

时采取措施加以解决。

第三,为了促进项目团队成员之间的协作与沟通,出海企业需要建立一套高效的沟通机制。这包括定期的项目审查会议、日常的工作汇报以及紧急情况的快速响应流程等。通过这些机制,出海企业可以确保信息的及时传递和问题的及时解决,从而提高整个项目的执行效率。

第四,考虑到跨境项目的特殊性,出海企业还需要特别关注文化差异对项目人员的影响。为此,出海企业可以提供跨文化培训,帮助项目人员了解不同文化背景下的工作习惯和沟通方式。这将有助于减少误解和冲突,提高团队协作的效率和质量。

第五,在跨境用工过程中,法律遵从也是一个不可忽视的问题。出海企业需要确保项目人员遵守当地法律法规,包括劳动法、税务和移民政策等。为此,出海企业可以与当地的法律顾问或专业机构合作,制定符合当地法律要求的用工计划和合同。

第六,为了降低潜在的法律和财务风险,出海企业还需要实施风险评估和管理计划。这包括对项目可能面临的法律、税务、汇率等方面的风险进行识别和评估,并制定相应的应对策略和预案。这将有助于出海企业在风险发生时迅速做出反应,减少损失和影响。

第七,为了支持项目人员的顺利工作,出海企业还需要提供必要的支持和资源。这包括培训、技术和行政支持等方面。出海企业将根据项目的具体需求和员工的个人发展要求来提供相应的支持,以确保项目人员能够充分发挥自己的才能和潜力。

综上所述,有效控制跨境项目人员需要出海企业采取一系列全面且细致的措施。通过制定明确的政策、采用先进的工具、建立高效的沟通机制、提供跨文化培训、确保合规性、实施风险评估和管理计划、建立绩效考核体系以及提供必要的支持和资源等,出海企业将能成功应对跨境用工中的挑战并取得优异的成绩。



第二篇 涉外劳动关系的识别及法律适用

一、涉外劳动关系的识别

对涉外劳动关系的识别,是正确适用中国劳动法律规范的关键,也是解决涉外劳动争议的前提和基础。涉外劳动关系可以从“劳动关系”和“涉外性”两方面加以识别。

(一)涉外“劳动关系”的认定

在处理涉外劳动关系时,“劳动关系”的确认首先需遵循劳动法的相关规定,即“劳动者”与“用人单位”必须满足法律设定的条件,这是构建“劳动关系”的基础。依据《劳动合同法》第7条:“用人单位从开始用工之日起即与劳动者确立劳动关系。”以及第10条第3款:“确立劳动关系时应签订书面合同,若用人单位与劳动者在用工前已签订劳动合同,则劳动关系自用工之日起生效。”因此,确认“劳动关系”的关键在于劳动者是否实际向用人单位提供了劳动,而书面劳动合同则是确立劳动关系的有力凭证。

相较于国内劳动者,国家对外国劳动者的劳动关系实施了更为严格的管理和控制措施。依据1996年劳动部、公安部等部委发布的《外国人在中国就业管理规定》(以下简称《规定》),外国人在中国就业必须先获得就业许可。根据《规定》第5条,外国人在华就业前必须取得就业证。此外,2013年最高人民法院《关于审理劳动争议案件适用法律若干问题的解释(四)》第14条明确指出:“未依法取得就业证件的外国人或无国籍人,以及未依法取得就业证件的香港特别行政区、澳门特别行政区和台湾地区居民,若与内地用人单位签订劳动合同,请求确认与用人单位存在劳动关系的,人民法院不予支持。”因此,若外国人在中国就业前未依法取得就业许可证,即便与用人单位签订了劳动合同并实际提供了劳动,也不能认定为涉外劳动关系。在司法实践中,此类情况通常按照一般劳务雇佣关系处理,依据《中华人民共和国民法典》进行,而非适用中国的劳动法律规范。

(二)涉外劳动关系中“涉外性”的判断

劳动关系是否具有“涉外性质”,决定了人民法院在审理劳动争议案件时,是否必须依据国际私法的冲突规范来确定适用的准据法(可能涉及外国法律,也可能涉及中国法律),抑或直接依据中国劳动法律规范来解决劳动争议。涉外劳动关系是涉外民事关系的一种类型,因此,识别劳动关系中的“涉外性质”可以从对涉外民事关系的认定入手。

根据1988最高人民法院《关于贯彻〈中华人民共和国民法通则〉若干问题的意见(试行)》的第178条规定:“凡民事关系的一方或双方当事人是外国人、无国籍人、外国法人的;民事关系的标的物在外国领域内;产生、变更或者消灭民事权利义务关系的法律事实发生在外国的,

均为涉外民事关系。”2013年1月7日实施的最高人民法院《关于〈中华人民共和国民事诉讼法〉若干问题的解释(一)》(以下称《法律适用法司法解释》)第1条则将“涉外民事关系”扩张至“民事关系的一方的经常居所地涉外”。

因此,在劳动关系领域,只要主体国籍、经常居所地、劳动者工作地、法律事实等要素涉及跨国因素,即可认定为涉外劳动关系。从司法实践的角度来看,涉外劳动关系可以根据劳动者的工作地点划分为两大类:首先,劳动者工作地在中国境内的涉外劳动关系。这包括中国企业与外国劳动者之间、外国企业在华分支机构与中国劳动者之间形成的劳动关系,以及外国劳动者受雇于外国企业后被派遣至中国境内的分支机构工作所形成的劳动关系。其次,劳动者工作地在境外的涉外劳动关系。这涵盖了外国企业与中国劳动者之间、中国企业与外国劳动者之间形成的劳动关系,其中劳动者的工作地点位于中国境外,以及中国人受雇于中国企业后被派遣至其境外分支机构工作所形成的劳动关系。

(三)与涉外劳动关系类似的法律关系

在司法实践中,存在一些与涉外劳动关系相似的其他法律关系。这些法律关系并不属于涉外劳动关系范畴,其法律适用规则与涉外劳动关系有所区别,因此必须将它们从涉外劳动关系中区分出来。

1. 中国公民受雇于外国企业的驻华代表处

根据中国法律规定,外国企业不得直接在中国境内开展经营业务,也不得直接招聘中国员工。外国企业必须通过其在中国设立的代表机构或分支机构,才能进行相关的商业活动。

外国企业在华设立的分支机构与代表机构在聘用中国员工方面存在差异。在华设立的分支机构可以依法招聘中国员工,提供劳动服务,而该分支机构与中国劳动者之间建立的劳动关系属于涉外劳动关系,其法律适用问题应按照涉外劳动关系的相关规定处理。然而,根据北京、广东、安徽等省市发布的《关于外国企业常驻代表机构聘用中国雇员管理规定》等地方性法规,外国企业常驻代表机构招聘中国雇员必须委托外事服务单位办理,不得私自或委托其他单位、个人进行招聘。中国公民必须通过外事服务单位向外国企业常驻代表机构求职应聘,不得私自或通过其他单位、个人到外国企业常驻代表机构求职应聘。外事服务单位应依照《中华人民共和国劳动法》与中国雇员签订劳动合同,并依法为中国雇员缴纳社会保险费用。

根据上述规定,外国企业驻华代表机构在中国境内不得与中国劳动者直接建立劳动关系。实际上,应由中国外事服务单位与中国劳动者签订劳动合同,再由中国外事服务单位与外国企业驻华代表机构签订提供劳动服务的合同。因此,中国劳动者与外国企业驻华代表机构之间不存在直接的劳动关系。中国劳动者只能与中国外事服务单位产生劳动争议。由于该劳动争议的主体、劳动者工作地均在中国境内,从国际私法的角度来看,这种劳动关系属于纯国内劳动关系,其法律适用问题无需依据《法律适用法》中关于涉外劳动关系的冲突规范来确定,而是应直接依据适用于国内劳动关系的法律进行处理。

2. 涉外劳务纠纷

在中国,劳动关系与劳务关系是两个不同的概念。劳动关系指的是合法的用人单位与劳

动者之间,为了实现劳动过程而形成的一种法律关系,其中一方有偿提供劳动力,而另一方则将其与自己的生产资料相结合。在劳动关系中,双方存在一定的从属关系,例如劳动者需将个人在一定范围内交付给用人单位。劳动者必须遵守劳动纪律,服从用人单位的管理,且劳动合同的内容不得规避法律的强制性规定。当劳动争议发生时,劳动法律规范将被用来进行调整。相比之下,劳务关系是指一方提供劳务,另一方有偿接受劳动成果而形成的法律关系。在劳务关系中,双方当事人的地位是平等的,劳务提供者自主管理,自由支配自己的劳动力,劳务需求者通常不进行管理和控制。一旦出现纠纷,这种劳务关系由民法和合同法进行调整。

在司法实践中,劳务关系通常分为两类:一类是个人之间的劳务关系。根据劳动法规定,劳动关系的一方必须是用人单位,因此,个人之间的劳务关系(如雇主与家庭保姆之间)不属于劳动法所指的劳动关系;另一类是不适格的用人单位与个人之间的劳务关系。如前所述,劳动法中的劳动关系必须存在于合法的用人单位与劳动者之间,如果用人单位和劳动者双方均不符合资格,则他们之间签订的合同不属于劳动合同,而是劳务合同。

因此,如在中国境内的外国人与被雇佣的家庭保姆之间形成的劳务关系,外国人未根据中国法律获得就业许可证而与用人单位建立的劳务关系,以及外国企业或其驻华代表机构与中国雇员建立的劳务关系,都不属于涉外劳动关系,而是属于一般的涉外劳务关系。此类涉外劳务关系一旦发生争议,当事人不必首先向劳动仲裁委员会申请仲裁,而可以直接向法院提起诉讼。其法律适用将根据《法律适用法》中关于一般涉外合同的冲突规范来确定,即合同当事人有权选择适用于涉外劳务关系的法律,而不是直接适用劳动者工作地的法律。

(四)法律适用对涉外劳动纠纷的影响

法律适用的不同对于涉外劳动纠纷的处理走向及裁判结果的影响重大,以周某与昕臆配件公司劳动纠纷一案(裁判文书案号为(2017)皖08民终466号)为例,周某与昕臆公司于2013年12月31日签订劳动合同,约定由昕臆配件公司安排周某至安哥拉工作,期限为两年,工资为每年100000元人民币。2014年1月至6月昕臆配件公司支付周某50000元。2014年7月至2015年7月,昕臆配件公司未向周某发放工资。2015年8月至2015年12月,周某到另一家汽车修理厂工作。后因昕臆配件公司欠付劳动报酬,遂发生纠纷。

本案的主要争议有三:(1) 本案适用我国法律还是安哥拉共和国法律;(2) 双方劳动关系终止时间的认定;(3) 周某主张拖欠的劳动报酬是否超过一年的时效。

在该法律文书中载明:“关于本案的法律适用问题。《中华人民共和国涉外民事关系法律适用法》第四条规定:‘中华人民共和国法律对涉外民事关系有强制性规定的,直接适用该强制性规定。’《最高人民法院关于适用若干问题的解释(一)》第十条规定……第十一条规定:‘一方当事人故意制造涉外民事关系的连结点,规避中华人民共和国法律、行政法规的强制性规定的,人民法院应认定为不发生适用外国法律的效力。’故本案应当适用中华人民共和国法律。”

我们认为(2017)皖08民终466号民事判决书主要存在以下问题:

1. 在一审法院的审理过程中,法律适用的问题未得到充分考虑。昕臆配件公司提出,其

与周某之间的劳动争议应依据安哥拉法律进行裁决,但一审法院未予采纳。相反,法院依据我国《劳动合同法》第50条以及《民事诉讼法》第65条和第142条作出了判决。然而,鉴于周某的工作地点位于安哥拉,本案涉及的是一个涉外劳动争议案件。因此,一审法院直接适用国内法律的做法并不妥当。

2. 在二审法院的判决中,未能明确阐述适用我国《法律适用法》第4条和《司法解释(一)》第10条的具体理由。一个完整的法律论证应当遵循典型的三段论结构,即法律条文作为大前提,案件事实作为小前提,通过这两者的综合分析,才能得出正确的结论。在这一过程中,任何一部分的缺失都将影响判决的质量。法官面临的挑战是如何在复杂且可能不完整的法律体系中,为具体案件找到恰当的法律依据,并进行合理的法律推理和论证,从而为案件的裁决建立适当的大前提。因此,判决书应当明确指出案件事实和争议点属于哪一法律规范的调整范围,并解释适用特定法律规则的理由。

3. 无须援引我国《司法解释(一)》第11条关于法律规避的规定。鉴于本案的准据法为我国法律,二审法院依据《法律适用法》第4条和《司法解释(一)》第10条直接适用我国法律,因此没有必要再适用《司法解释(一)》第11条。实际上,如果准据法为外国法律,即便法律规避和强制性规范的适用条件都已满足,也应优先考虑强制性规范的适用。

4. 以法律规避为由排除当事人选择适用的安哥拉国法律的做法并不恰当。法律规避制度与涉外民事关系法律适用法中的当事人意思自治原则存在冲突。从法律效果的角度来看,当事人的意思自治和法律规避都导致了本应适用的法律的改变,这使得原本指向的准据法无法适用,这一点不容忽视。区别在于,法律规避行为必须具备“故意”的欺诈性。^[1]然而,“故意”是一种心理状态,需要有充分的证据来证明。而作为法律规避对象的强制性规则,通常指的是国内法上的强制性规定。在本案中,双方当事人既没有表现出“故意”的欺诈性,也没有违反我国的强制性规范,因此法院不能以法律规避为由排除适用当事人选择的安哥拉国法律。

因此,对于本案中劳动关系的终止时间问题和时效问题,应当采取分割方法,分别根据《法律适用法》第43条和第7条确定应适用的准据法。

根据以上内容可知,对于法律适用的选择,对案件管辖权确定、案件的审理具有直接的影响。

二、涉外劳动纠纷中法律适用的常见情形及利弊分析

(一)涉外劳动纠纷适用的一般规定

在处理跨国劳动关系时,由于涉及的主体和劳动者工作地点的国际性质,可能会出现因社会制度和文化差异而产生的保护劳动者权益观念上的冲突。因此,与国内劳动关系相比,跨国劳动关系及其法律规制更为复杂。近年来,跨国劳动争议案件数量急剧上升,但现行立

[1] https://m.sohu.com/a/417565476_120051855/

法尚未充分关注这一特殊法律关系。现有的涉外劳动法律规范往往含糊不清,并且存在相互矛盾的情况。

当跨国劳动合同当事人之间发生劳动争议并诉诸法院时,由于劳动争议的跨国性质,法院应依据法院地国的冲突规范来决定适用的准据法,而不是直接依据法院地的劳动法律规范进行处理。根据中国《法律适用法》第43条的规定:“劳动合同适用劳动者工作地法律;若难以确定劳动者工作地,则适用用人单位的主营业务地法律。劳务派遣情况下,可以适用劳务派遣地法律。”该条款属于双边冲突规范。据此,如果劳动者的工作地点在中国境内,涉外劳动争议可以适用中国的劳动法律规范解决;若劳动者的工作地点在境外,则应适用相关外国的劳动法律规范来处理。然而,当劳动者工作地在境内时,如果涉外劳动合同中当事人的约定与中国劳动法律规范中的强制性规定相冲突时,是否一律导致其约定无效?或者当劳动者的工作地在境外时,中国劳动法律规范中的强制性规定是否一律不能加以适用?

(二)属地——工作地在境内的劳动纠纷法律适用

劳动法律规范中包含任意性规定和强制性规定。任意性规定允许劳动合同当事人通过协议进行调整。例如,《劳动法》第21条前半段指出:“劳动合同可以约定试用期”,这便是一条任意性规定,是否在合同中设定试用期由当事人自行决定,即便不设定试用期,也不会影响合同的有效性。识别劳动法律规范中的任意性规定,可以通过法条中的“关键词”来判断,如法律条文中的“可以”一词通常表示任意性规定。例如,对于劳动合同必备条款之外的其他条款、保守商业秘密的约定、福利待遇的规定,以及劳动合同的协议解除等,都属于任意性规定。在涉外劳动合同中,若当事人有其他约定,法院应尊重当事人的自主意愿。

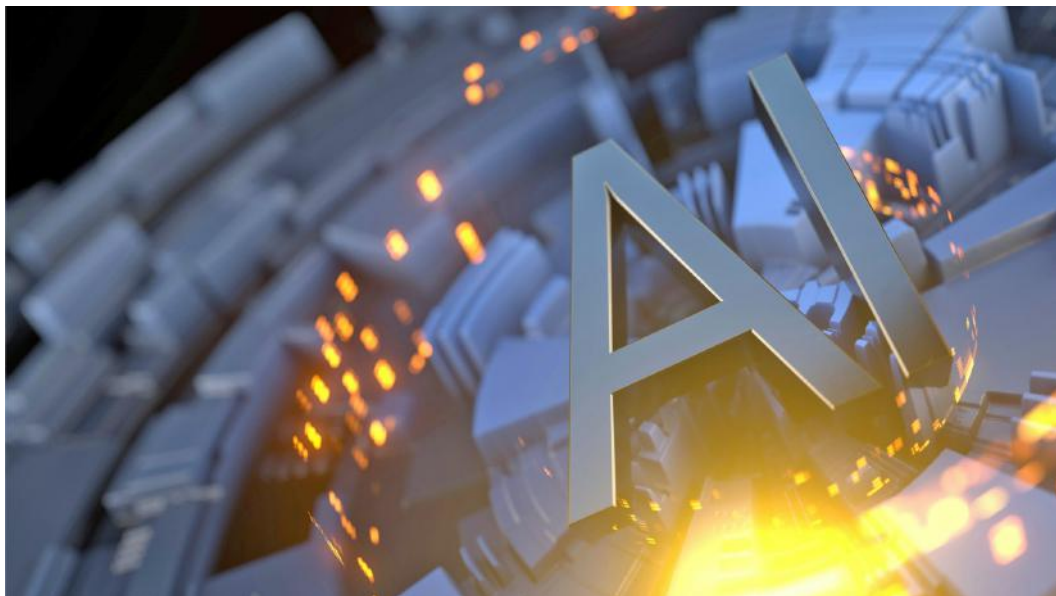
除了任意性规定,为了保护劳动者这一弱势群体的合法权益,劳动法律规范中还设有大量强制性规定。在纯国内的劳动合同中,如果当事人通过协议规避这些强制性规定,可能会导致合同部分或全部无效,并且当事人可能需要承担行政甚至刑事责任。这些强制性规定通常在劳动法律规范中通过含有“必须”“不得”“禁止”“应当”等关键词的法律条文体现,例如关



于最长工作时间、最短休息时间、最低带薪年假、最低工资标准、健康和职业安全、妇女和青少年的保护措施、男女平等、同工同酬以及禁止歧视、无固定期限劳动合同的签订、用人单位单方解除劳动合同的条件等。

劳动法律规范中的所有强制性规定是否自动适用于在中国境内履行的涉外劳动合同,这是一个复杂的问题。如前所述,境内履行的涉外劳动合同大致分为三种类型。对于外国企业在华分支机构与中国劳动者签订的、工作地点在中国境内的劳动合同,从保护劳动者权益的角度出发,劳动法律规范中的所有强制性规定都应适用,这一点在理论和实务界已达成共识。然而,对于外国劳动者受雇于外国企业后被派往中国境内分支机构工作,以及中国企业与外国劳动者在中国境内工作的情形(这两类统称为“外国人在华就业”),中国劳动法律规范中的强制性规定是否必须适用,在司法实践中存在较大争议,有必要进行深入分析。

1. 劳动基准的强制性规定适用性。劳动基准,又称劳动标准,有广义和狭义之分。广义的劳动基准包括两个方面:一是劳动条件水平的标准;二是强制性劳动关系运行规则。狭义的劳动基准仅指劳动条件基准,即用人单位必须提供给劳动者的最低劳动条件,包括工资、工作时间、休息休假、女职工和未成年工保护、劳动安全卫生以及社会保险等最低标准。本文所指的劳动基准采用狭义定义。《劳动法》和《劳动合同法》均对这些劳动基准作出了强制性规定。1996年《规定》第23条明确指出:“在中国就业的外国人的工作时间、休息、休假、劳动安全以及社会保险应按照国家有关规定执行。”因此,外国人在华就业时,用人单位必须遵守中国劳动法律规范所规定的最低标准。实践中,外国人在华就业的最低工资标准、最长工作时间、休息休假、劳动卫生与安全等标准或待遇,各地都能严格按照劳动法律规范的强制性规定执行。然而,在外国就业人员参加社会保险的时间上,各地存在先后差异,标准不一,导致在华就业的外国人参加社会保险制度较为混乱。为此,国家人力资源和社会保障部于2011年发布了《在中国境内就业的外国人参加社会保险暂行办法》,该办法明确了在中国境内就业的外国人参加社会保险的条件和要求,并规定了用人单位或境内工作单位未依法为招用的外国人办理社会保险登记或未依法为其缴纳社会保险费的法律责任,以确保外国人在华就业时的



合法权益得到维护。

2. 其他强制性规定的适用性。从上述分析可知,劳动基准的强制性规定适用于在中国履行的涉外劳动合同。但是,其他强制性规定,如劳动合同的违约责任、无固定期限合同的签订,特别是用人单位单方解除劳动合同的条件等,是否也应适用,还是允许外国人与用人单位自由约定?上海市劳动局1998年发布的《关于贯彻〈外国人在中国就业管理规定〉的若干意见》(以下简称《意见》)第16条规定:“用人单位与获准聘雇的外国人之间有关聘雇期限、岗位、报酬、保险、工作时间、解除聘雇关系条件、违约责任等双方的权利义务,通过劳动合同约定。”该条成为上海地区人民法院裁决此类劳动合同纠纷的主要依据。例如,在“陈德基诉飞世尔试验器材制造(上海)有限公司的劳动合同纠纷”一案中,上海南汇区人民法院根据《意见》第16条的规定认为,用人单位与外国人之间有关解除聘雇关系的双方权利义务,可以由双方通过劳动合同约定,从而驳回了原告要求继续履行合同的主张。上海地区法院支持当事人在单方解除合同条件上的意思自治,即使约定的解除条件与法律的强制性规定不同。

然而,北京地区的人民法院对此持有相反的理解。他们认为,劳动合同的约定不能违反法律的强制性规定。对于用人单位单方解除劳动合同的条件,劳资双方虽然可以约定,但这个约定的解除条件不能低于劳动法和劳动合同法保护的强制标准。劳动合同法对于用人单位单方解除权的限制性规定,是劳动者在这个方面受保护的最低标准。因此,劳动合同约定的保护水平不能低于该标准。

(三)属人——工作地在境外的劳动纠纷法律适用

在处理劳动者工作地点位于境外的涉外劳动关系时,依据《法律适用法》的规定,原则上应适用劳动者工作地的法律,即外国法律。然而,这是否意味着此类劳动合同纠纷完全不能依据中国劳动法律规范来解决呢?《法律适用法》第4条明确指出:“中华人民共和国法律对涉外民事关系有强制性规定的,直接适用该强制性规定。”这一条款确立了国内法中强制性规定在涉外民事关系中的直接适用性。换言之,无论冲突规范确定的准据法为何,亦或当事人选择的准据法为何,这些强制性规定都必须在涉外民事关系中得到直接适用。

为了帮助各级法院在审理涉外民商事案件时正确应用这些“强制性规定”,最高人民法院于2013年发布的《法律适用法司法解释》第10条,对“强制性规定”的范围进行了明确列举。其中,第一款就包括了涉及劳动者权益保护的强制性规定。因此,当劳动者工作地点在境外的劳动合同纠纷被诉至中国法院时,国内法中涉及劳动者权益保护的强制性规定有可能在这些涉外劳动纠纷中得到直接适用,即便根据冲突规范确定的准据法为外国法。

然而,并非所有国内法中涉及劳动者权益保护的强制性规定都能在涉外劳动关系中撇开冲突规范而直接适用。国际私法的核心原则是根据冲突规范指引确定的准据法应当得到适用,即便有时这意味着牺牲国内法上的某些强制性规定。^[2]那么,在中国劳动法律规范中,哪些强制性规定可以适用于涉外劳动关系呢?只有那些旨在保护国家根本利益和社会公共利益的强制性规定才能在涉外劳动关系中得到直接适用。例如,《劳动合同法》第14条规定,雇

[2] <https://baijiahao.baidu.com/s?id=1668270607243240126>

主和雇员连续签订两次固定期限合同后,雇员有权要求签订无固定期限合同。该规定旨在遏制劳动合同短期化趋势,反映了政府的政策倾向。但是,该规定不能在涉外劳动关系中撇开冲突规范确定的外国法而直接适用,因为它并不涉及中国政府的根本利益或公共利益。

在劳动法律规范中,只有与劳动基准相关的强制性规定才能在涉外劳动关系中直接适用。这些与劳动基准相关的强制性规定是国家基于维护作为弱势群体的劳动者生存权,进而维护整个社会安全的需要,对劳动关系进行干预。对弱势群体的倾斜保护有助于实现社会实质公平,增进公共利益,保护的不仅是劳动者个人利益,更是社会的整体利益。因此,在审理涉外劳动纠纷案件时,如果根据冲突规范指引的外国法,其对劳动者的保护标准低于中国劳动法律规范中的最低标准,法院可以忽略外国法的适用,直接适用中国的强制性规定。

三、如何在涉外劳动争议中适用中国劳动法律规范

在处理涉外劳动争议时,为了确保能够妥善且合法地适用中国劳动法律规范,我们建议出海企业应当从以下几点出发:

第一,明确管辖权的归属是至关重要的第一步。出海企业需仔细审视争议双方的法律地位以及争议行为的发生地,确保中国劳动法律对此类争议具有明确的管辖权。这一步骤不仅要求我们具备扎实的法律知识,还需要出海企业对案件事实有深入的了解和把握。

第二,深入理解并全面掌握中国劳动法律的相关规范是处理涉外劳动争议的基础。从《中华人民共和国劳动法》到《中华人民共和国劳动合同法》,再到相关的司法解释和行政规章,每一项法律条款都需我们细细研读,确保在处理争议时能够准确无误地援引法条。同时,出海企业还应关注法律的动态变化,及时更新知识储备,以应对可能出现的法律挑战。

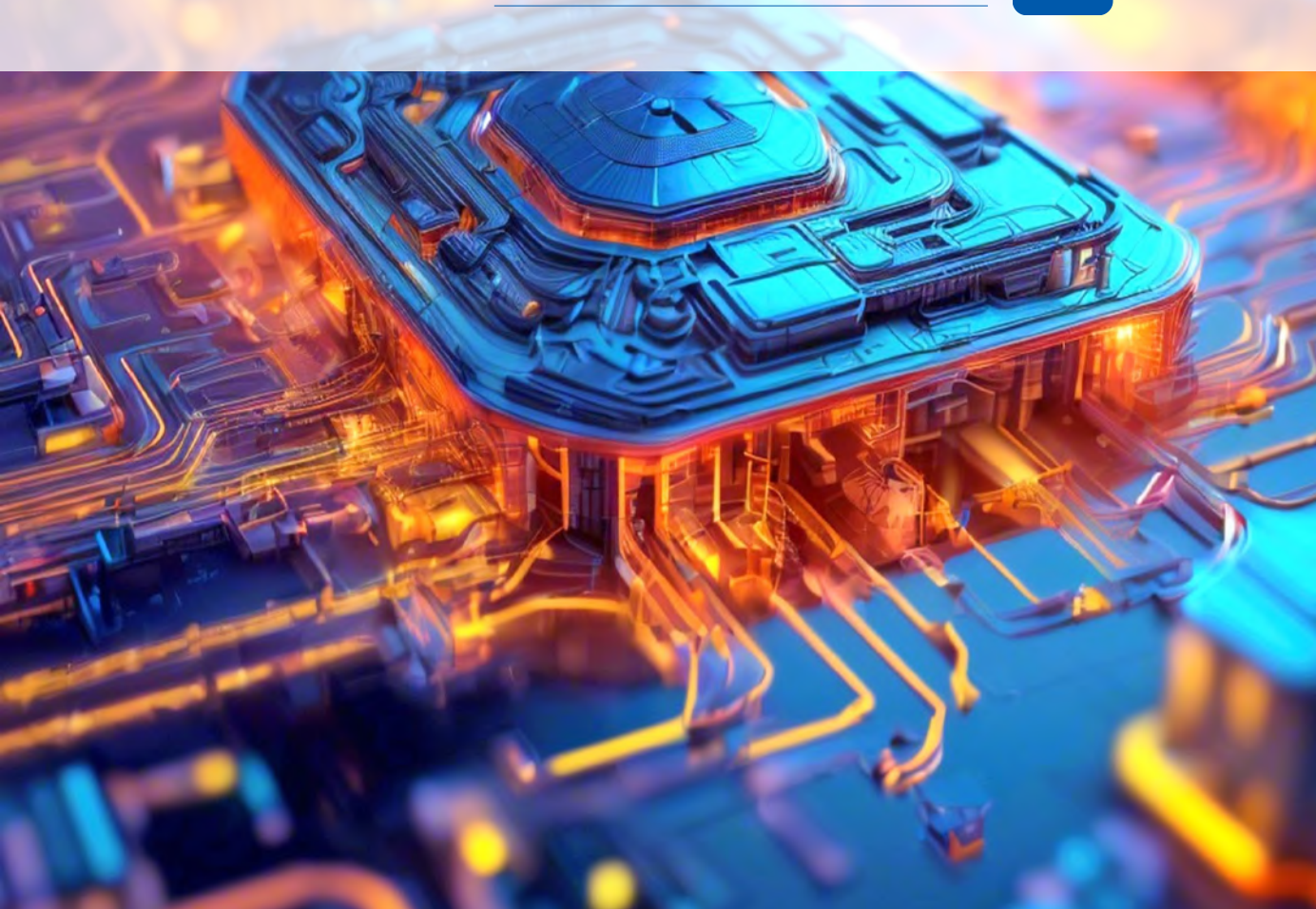
第三,在劳动合同方面,合同条款的审查同样不容忽视。出海企业需仔细审视合同中关于争议解决方式、适用法律以及争议解决地点的条款,确保其符合中国法律的规定。如果发现合同条款存在瑕疵或不合规之处,出海企业应及时提出并建议进行修改或补充,以避免在争议解决过程中陷入被动。

第四,证据是应对劳动仲裁与诉讼的重中之重。实践中在人资双方在无明确的纠纷管辖约定以及其他管辖强制性规范情况下,存在不少的案例是根据劳动者一方提供的证据材料确定劳动行为给付地(劳动合同履行地)或当地裁判机构能够以证据认定是否具有案件管辖权的。因此,出海企业应当重视文档证据的收集和整理,需全面收集与争议相关的文件和证据,包括但不限于劳动合同、工资单、工作记录、邮件往来等。在收集过程中,出海企业需确保证据的真实性和完整性,以便在争议解决过程中为企业的主张提供有力支撑。



人工智能产品 法规遵从

第四章



第一篇 全球人工智能法规概览

一、欧盟《人工智能法案》及成员国法规

(一) 欧盟《人工智能法案》的主要内容及影响

欧盟《人工智能法案》(AI Act)于2021年4月由欧盟委员会提议,并于2023年12月得到欧洲议会和理事会的批准,于2024年8月正式生效。法案旨在应对人工智能技术在快速发展中可能带来的潜在风险,如对欧盟公民健康、安全和基本权利的威胁,其通过提供统一的框架来规范人工智能的开发和部署,在确保技术的安全性和透明度的同时,促进创新并减少企业的行政和财务负担。

欧盟《人工智能法案》采用了基于风险的分级监管框架,将人工智能系统分为四个风险类别:不可接受风险、高风险、特定透明度风险和最低风险,意在人工智能系统的潜在风险程度实施相应的监管措施。

不可接受风险:包括能够进行社会评分的人工智能系统,类似系统被认为会对人权构成威胁,因此在欧盟境内被全面禁止。

高风险:包括用于招聘、教育、公共服务等关键领域的人工智能系统。类似系统需要满足严格的合规要求,包括建立风险管理系统、实施数据治理、准备技术文档和提供用户信息等,以确保系统的安全性和可靠性。具体来说,高风险人工智能系统的提供商必须进行数据质量管理,确保数据集的代表性和准确性,同时设计系统以实现人类监督和系统的安全性与鲁棒性。

特定透明度风险:此类人工智能系统要求提供明确的用户通知,例如聊天机器人需要告知用户他们正在与人工智能进行互动。

最低风险:如人工智能驱动的游戏和垃圾邮件过滤器,对此类系统没有强制性的监管要求,企业和开发者可以自由使用,但鼓励他们自愿遵循额外的行为准则,以提高系统质量和用户信任。

欧盟《人工智能法案》作为全球首部全面规范人工智能技术的法律,预计将在多个层面产生深远影响。

欧盟内部影响:该法案旨在通过严格的监管框架提高人工智能系统的安全性和公众信任,从而促进创新和经济增长。企业,尤其是涉及高风险人工智能系统的企业,将需要适应新的合规要求,这可能会增加运营成本,但也将推动更高标准的技术开发。

全球影响:欧盟《人工智能法案》可能成为其他国家制定人工智能法规的基准。其他国家如美国、英国等也在密切关注欧盟的这一举措,并评估其适用性和效果。国际企业可能会根

据该法案调整其全球人工智能策略,以避免在不同市场之间的合规冲突。该法案可能推动国际合作与标准化进程,促进全球人工智能治理框架的形成,其不仅有助于解决跨境人工智能应用的监管问题,还可能推动全球在人工智能伦理、安全和隐私保护等方面达成共识。

(二)欧盟成员国的人工智能相关法规概览

欧盟《人工智能法案》为成员国提供了统一的监管框架,但各成员国也在积极制定和完善本国的人工智能法规。

德国作为欧盟的经济引擎,在人工智能治理领域走在前列,2018年,德国发布《德国联邦政府人工智能战略》(The Artificial Intelligence Strategy of the German Federal Government),提出“AI Made in Germany”口号,将人工智能发展提升到国家战略高度。同年成立的数据伦理委员会在2019年发布了75项人工智能和数据伦理建议,提出数据和算法协同治理、分级监管等理念。德国还在自动驾驶、著作权等方面完善了相关法律。

法国则于2022年通过《人类为本的人工智能法》(Human-Centric Artificial Intelligence Act),要求对高风险人工智能进行影响评估,禁止社会评分,要求人工智能决策透明化。法国国家信息与自由委员会(National Commission on Informatics and Liberty, CNIL)在2023年发布了人工智能系统发展建议,明确了《人工智能法案》与《通用数据保护条例》(GDPR)的关系。

丹麦则聚焦公共部门人工智能应用,其数据保护局于2023年发布了公共机构开发和和使用人工智能的指南,强调数据保护、公民权利和透明度。

这些成员国的法规总体上与欧盟《人工智能法案》保持一致,都强调基于风险的分级监管、伦理原则和个人数据保护。同时,各国法规在某些方面对《人工智能法案》进行了补充和细化。例如,德国提出的5级风险评级制度,法国对人工智能训练数据的知识产权保护,以及丹麦对公共部门人工智能应用的具体指导。《人工智能法案》允许成员国在某些领域(如国家安全)制定更严格的规则,这为各国根据自身情况进行调整提供了空间。各国也在建立或完善本国的人工智能监管机构,如法国国家信息与自由委员会(National Commission on Informatics and Liberty, CNIL)、德国的数据伦理委员会(Datenethikkommission, DEK)等,以配合欧盟层面的监管框架。

值得注意的是,2023年11月,德国、法国和意大利三国政府联合提出了关于人工智能监管的建议,主张欧盟相关企业在人工智能应用上作出具有约束力的自愿承诺。这一建议反映了成员国之间在人工智能监管方面的协调努力,有助于推动欧盟整体监管框架的完善。

总的来说,欧盟成员国在制定本国人工智能法规时,既遵循了欧盟《人工智能法案》的总体框架,又根据各自国情进行了创新和补充。这种“统一中的多样化”路径有助于在保持监管一致性的同时,促进人工智能技术和应用的创新发展。

(三)欧盟其他人工智能相关标准与指南

除《人工智能法案》外,欧盟还制定了一系列补充性标准和指南,以构建更全面的人工智能治理框架。上述举措旨在平衡创新与监管,确保人工智能技术的安全、可靠和负责任发展。

《人工智能责任指令》(Artificial Intelligence Liability Directive, AILD), 欧盟委员会于2024年9月提出了适应非合同性民事责任规则以应对人工智能发展的《人工智能责任指令》。该指令旨在填补现有法律在应对生成式人工智能带来的特定风险(如歧视和侵犯人格权)方面的空白。AILD与《人工智能法》和修订后的《产品责任指令》(Product Liability Directive, PLD)共同构成欧盟针对人工智能系统的全面义务和责任框架。

AILD的主要特点包括采用《人工智能法》中的关键概念,确保法律连贯性;引入“高影响人工智能系统”概念,涵盖高风险和附加系统;建立证据披露义务和与过错及因果关系有关的可反驳推定;对禁止使用的人工智能系统实施严格责任;以及考虑将通用人工智能系统纳入管辖范围。

《人工智能公约》(EU AI Pact), 2024年9月, 欧盟委员会公布了《人工智能公约》, 该公约是一项旨在促使企业就人工智能处理和部署发布“自愿承诺”的倡议。目前欧盟委员会公布的签署方名单覆盖面极广, 囊括了电信公司、咨询公司软件公司、银行/支付公司跨国公司、中小企业和面向消费者的平台, 如亚马逊、微软、OpenAI、谷歌等。前述公约鼓励组织提前规划, 以落实《人工智能法》的相关措施。公约围绕两个支柱构建: 一是建立《人工智能公约》网络, 鼓励交流最佳实践, 提供关于《人工智能法》实施的实用信息; 二是鼓励人工智能系统的提供者和部署者提前采取措施, 遵守立法要求和义务。

参与公司承诺至少采取三项核心行动: 采用人工智能治理战略, 促进组织内部人工智能的采用; 识别和梳理可能被归类为高风险的人工智能系统; 在员工中推广人工智能意识和知识, 确保道德和负责地开发人工智能。为进一步完善人工智能治理框架, 欧盟正在考虑制定统一的软件责任法规, 以覆盖所有类型的软件, 包括人工智能和非人工智能软件。上述法规可能以条例的形式呈现, 以确保所有软件应用程序都能统一适用可反驳推定和证据披露机制。

以上所说的补充性标准和指南反映了欧盟在人工智能治理方面的全面思考, 旨在建立一个平衡创新、保护消费者权益、确保法律清晰度的监管环境。通过前述措施, 欧盟希望在促进人工智能技术发展的同时, 有效管控其潜在风险, 为全球人工智能治理提供参考模式。

二、美国人工智能相关标准、规则与法案

(一) 美国联邦层面的人工智能立法及展望

美国联邦层面的人工智能法律和规则制定呈现出“软法治理”与“逐步趋硬”的特点。2021年, 美国通过《2020年国家人工智能倡议法案》(National Artificial Intelligence Initiative Act of 2020), 正式成立国家人工智能倡议办公室, 负责实施国家人工智能战略。2022年, 白宫科技政策办公室(Office of Science and Technology Policy, OSTP)出台《人工智能权利法案蓝图》(Blueprint for an AI Bill of Rights), 明确了创建安全有效系统、应对算法歧视、保护数据隐私等五项关键原则。2023年, 国家标准与技术研究所(National Institute of Standards and Technology, NIST)发布《人工智能风险管理框架》(Artificial Intelligence

Risk Management Framework, AI RMF), 为人工智能创新生态系统的设计、开发和部署提供指导。上述举措体现了美国政府在推动人工智能发展的同时, 也在逐步建立监管框架。

面对生成式人工智能带来的潜在风险, 美国政府开始采取更积极的监管态度。2023 年 7 月, 美国政府和七家人工智能巨头达成“自愿承诺”, 旨在确保人工智能技术的安全、可靠和透明发展。10 月, 拜登总统签署了《关于安全、可靠和可信赖人工智能的行政命令》(Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence), 要求多个政府机构制定标准以防止人工智能被用于设计生物或核武器等威胁, 并要求公司在训练强大的基础模型时通知政府并分享安全测试结果。

在具体法案方面, 美国国会也在积极推进。2022 年, 多位参议员提出了《2022 年算法责任法案》(Algorithmic Accountability Act of 2022, H.R. 6580), 旨在提升算法应用的普及性、精准性及透明度。2023 年, 国会通过了《内容来源保护和防止编辑和深度伪造媒体完整性法案》(Content Origin Protection and Integrity from Edited and Deepfaked Media Act, COP-IED), 以解决人工智能生成内容的“深度伪造”问题。多个委员会还通过了一系列人工智能相关法案, 如《创造人工智能法案》(Creating Resources for Every American To Experiment with Artificial Intelligence Act of 2023, CREATE AI Act of 2023)《国家科学基金会人工智能教育法案》(National Science Foundation AI Education Act of 2024, NSF AI Education Act of 2024)等。

(二)美国各州人工智能立法动态及特点

美国各州在人工智能立法方面正呈现出积极推进、各有侧重的特点。加利福尼亚州、犹他州和科罗拉多州等率先出台了相关法案, 为其他州乃至联邦层面的人工智能监管提供了宝贵经验。

2024 年 8 月, 加利福尼亚州通过了《前沿人工智能模型安全可靠创新法案》(Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, SB-1047), 成为美国首个针对大规模人工智能模型进行监管的州。该法案明确针对前沿模型, 设置了“严重损害”的责任红线, 要求开发方具备“一键关停”能力, 并规定了开源模型的风险责任和第三方审计要求, 体现了加州在人工智能监管方面的前瞻性思维, 旨在平衡创新与安全。

紧随其后, 犹他州于 2024 年 5 月 1 日正式实施《犹他州人工智能政策法》(Utah Artificial Intelligence Policy Act, UAIPA), 成为美国首个颁布专门管理人工智能服务消费者保护法规的州。该法案的特点在于其全面性, 不仅明确定义了关键概念, 还区分了受监管主体和非受监管主体的义务, 设立了人工智能政策办公室, 并创立了人工智能学习实验室项目。犹他州的做法展现了一种综合性的监管思路, 既注重保护消费者权益, 又为人工智能创新预留了空间。

科罗拉多州则于 2024 年 5 月 17 日签署通过《科罗拉多州人工智能法案》(Colorado Artificial Intelligence Act, SB 24-205), 计划于 2026 年 2 月 1 日生效。该法案的重点放在防止算法歧视上, 特别是在就业等关键决策领域。它明确定义了“高风险人工智能系统”, 对开发者和部署者提出了具体的责任和义务, 要求进行定期影响评估和风险管理。科罗拉多州的做

法体现了对人工智能应用中潜在社会问题的关注,为其他州在处理人工智能公平性问题上提供了参考。

尽管各州的立法重点有所不同,但它们都体现出了一些共同特点:注重风险管理、强调透明度、保护消费者权益、平衡创新与监管,以及关注特定高风险应用领域。这些立法反映了各州对人工智能技术潜在影响的深刻认识,以及在监管框架下促进创新的决心。但同时,各州在执法机制和具体措施上也存在差异,如犹他州设立专门的人工智能政策办公室,而科罗拉多州则赋予总检察长新的职能。

(三) 美国人工智能标准与行业自律规范

美国在人工智能领域的标准制定和行业自律规范正在快速发展,体现了政府、行业和学术界的共同努力。这些措施旨在促进人工智能技术的安全、可靠和负责任地发展,同时保持美国在全球人工智能竞争中的领先地位。

首先,美国国家标准与技术研究院(NIST)于2023年1月发布的人工智能风险管理框架(AI RMF)是一个重要的里程碑。这个自愿性框架围绕治理、映射、衡量和管理四个核心功能构建,为各类组织提供了管理人工智能相关风险的综合指南。该框架的灵活性使其适用于不同规模和行业的组织,体现了美国在人工智能标准制定方面的前瞻性思维。

在特定领域的人工智能应用中,美国联邦航空管理局(FAA)于2024年7月发布的《人工智能安全保证路线图》(Roadmap for Artificial Intelligence Safety Assurance)是另一份重要的标准文件,其不仅关注如何确保人工智能在航空领域的安全应用,还探讨了如何利用人工智能技术提高航空安全。

在网络安全领域,美国国土安全部网络安全和基础设施安全局(Cybersecurity and Infrastructure Security Agency, CISA)发布的《降低人工智能风险:关键基础设施所有者和运营者功能安全和网络安全指南》(Safety and Security Guidelines for Critical Infrastructure Owners and Operators)为保护关键基础设施免受人工智能相关威胁提供了重要指导。指南强调了组织文化、风险评估和持续监控在管理人工智能风险中的重要性。

在行业自律方面,2023年7月21日,拜登总统与七大科技公司领导人达成的自愿框架是一个重要的里程碑。这个被称为“7月21日框架”的倡议包括了安全、保障和信任三个方面的八项承诺。尽管是一个自愿性框架,但它代表了行业领袖们对负责任人工智能发展的承诺,也体现了政府在推动人工智能自律方面的积极作用。

三、其他主要国家与地区性法规

(一) 英国人工智能监管框架与政策举措

英国在人工智能监管框架和政策举措方面展现了独特的灵活性和前瞻性。2023年,英国政府发布了《促进创新的人工智能监管方式》(AI Regulation: A Pro-Innovation Approach)政策文件,明确将监管目标定位为“提供清晰的、有利于创新的监管环境”。政策强调

“按比例监管”的灵活方式,旨在推动英国成为“世界上建立基础人工智能企业的最佳地点之一”。同时,英国还发布了《建立有效人工智能认证生态系统的路线图》(The Roadmap to an Effective AI Assurance Ecosystem),致力于培育包括影响评估、偏见审计、认证和性能测试等在内的中立第三方服务体系,力图在全球人工智能认证行业中占据领先地位。

在具体实施层面,英国各相关部门也积极行动。2023年4月,英国信息专员办公室(ICO)发布了针对人工智能生成内容的开发和使用指南,明确列出了八大重点关注领域,包括处理个人数据的合法依据、数据保护影响评估以及限制不必要处理等内容。同年3月,英国政府在《促进创新的人工智能监管方式》(AI Regulation: A Pro-Innovation Approach)中将问责和管理原则列为五项核心原则之一,这一原则同时也是英国数据监管机关在监管人工智能使用和生成个人数据方面的重点,体现了英国在保护个人隐私和数据安全方面的能力和要求。

2023年11月23日,克里斯-霍姆斯勋爵向英国上议院提交的《人工智能(监管)法案》(Artificial Intelligence (Regulation) Bill)标志着英国人工智能监管框架的进一步完善。该法案可视为落实《人工智能白皮书》以及实现英国在近期人工智能峰会上发布的《布莱切利宣言》(The Bletchley Declaration)承诺的重要一步。法案授权国务大臣成立专门的人工智能管理局,负责协调和实施监管工作。该管理局的职能广泛,包括确保其他监管机构考虑人工智能因素、进行监管差距分析、监测人工智能相关风险,以及促进与国际监管框架的互操作性等。这一法案的提出,加上英国于2023年11月1日至2日在布莱切利园主办的首届全球人工智能安全峰会,充分体现了英国在全球人工智能治理中的领导地位和积极贡献。

(二)新加坡人工智能治理工具与指南

新加坡在人工智能治理领域一直走在全球前列,展现了独特的前瞻性和系统性。2019年1月,新加坡发布了亚洲首个人工智能模型治理框架(草案)(Model Artificial Intelligence (AI) Governance Framework),并于2020年1月发布了第二版。这个框架围绕两个核心原则展开:确保人工智能决策的可解释性和透明度,以及坚持以人为本的人工智能应用。同年11月,新加坡又发布了《国家人工智能战略》(National Artificial Intelligence Strategy, NAIS),设定了到2030年成为人工智能广泛应用的智慧国家的宏伟目标。这些早期举措为新加坡在人工智能领域的长远发展奠定了坚实基础。

在实践层面,新加坡政府采取了一系列创新措施。2022年5月,新加坡推出了全球首个人工智能治理评估框架和工具包——AI Verify,旨在帮助企业对人工智能系统进行自我评估,验证其性能和可信度。2023年12月,新加坡更新了《国家人工智能战略2.0》(National Artificial Intelligence Strategy 2.0, NAIS),进一步明确了未来三到五年的发展方向。2024年1月,新加坡AI Verify基金会(AIVF)和信息通信媒体发展局(IMDA)共同制定了《生成式人工智能治理的模型人工智能治理框架草案》(Draft Model AI Governance Framework for Generative AI),专门针对生成式人工智能的治理问题提供指导。这些举措体现了新加坡在人工智能治理领域的持续创新和与时俱进。

(三)日、韩人工智能法规特点

日本的人工智能法规体系展现出了“软法治理”与国际合作的鲜明特征。2019年发布的《人工智能以人为本的社会原则》(Social Principles of Human-Centric AI)奠定了日本人工智能治理的基调,强调以人为本、尊重人权、确保隐私和安全等核心价值。2021年的《人工智能治理报告》(AI Governance in Japan Ver. 1.0)进一步体现了日本倾向于采用非约束性指导而非严格法规的治理方式,提倡敏捷治理和多方利益对话。这种灵活的方法旨在适应人工智能技术的快速发展,同时鼓励企业自主治理。在国际合作方面,日本通过2023年启动的“广岛人工智能进程”(Hiroshima AI Process)积极推动全球人工智能治理标准的制定,展现了其在国际人工智能治理中的领导意愿。此外,日本在人工智能版权问题上采取了相对开放的态度,如2024年1月发布的人工智能与版权指南草案(Draft AI Guidelines for Business)允许在不需要额外同意的情况下将受版权保护的作品用于人工智能训练,有利于人工智能技术的创新发展。

相比之下,韩国的人工智能法规体系呈现出更为全面和具体的特点,注重制度化和法律保障。2020年发布的《改进人工智能法律、制度和监管的路线图》(Roadmap for Improving AI Law, System and Regulation)为韩国建立系统性的人工智能法律框架奠定了基础。2023年的《数字权利法案》(Digital Bill of Rights)进一步明确了数字时代公民的基本权利,包括对人工智能决策的解释权和选择退出权,体现了韩国在保护公民数字权利方面的决心。在具体实践中,韩国通过制定《可信赖人工智能的集体工业标准》(Industrial Standards for Trustworthy AI)和《人工智能服务用户保护法》(AI Service User Protection Act)等措施,对人工智能系统的全生命周期进行规范,包括风险管理、透明度和问责制等方面。

(四)香港特别行政区人工智能政策与监管框架

香港特别行政区在制定人工智能监管指南和框架方面近期取得了显著进展,尤其聚焦于数据保护和道德使用等关键领域,其中多个政府机构发布的若干框架和指南构成了上述进展的核心内容。

在主要指南和框架方面,香港个人资料私隐专员公署(Office of the Privacy Commissioner for Personal Data, PCPD)于2024年发布的《人工智能:个人资料保障模范框架》(Artificial Intelligence: Model Personal Data Protection Framework)为涉及个人数据的人工智能系统使用组织提供了实用建议。该框架着重强调了人工智能系统的道德采购、实施和使用,在适当的人工监督下进行风险评估,建立内部人工智能治理委员会,以及最小化收集用于训练人工智能模型的个人数据等关键方面,旨在确保符合《个人资料(私隐)条例》(第486章)的规定。虽不具法律约束力,但为人工智能部署的最佳实践提供了重要指导。

此外,香港个人资料私隐专员公署(Office of the Privacy Commissioner for Personal Data, PCPD)于2021年还发布了关于人工智能道德开发和使用的指导,其中包括责任、透明度和公平性等原则。该指导针对开发人工智能解决方案的组织,是对前述模范框架的有力补充。与此同时,香港金融管理局(Hong Kong Monetary Authority, HKMA)也发布了关于在

面向客户的应用中使用生成式人工智能的具体指南。上述指南侧重于消费者保护,概述了授权机构在其运营中实施人工智能技术时必须遵循的原则。

就监管格局而言,香港目前尚未建立专门管理人工智能的综合法律框架,然而,各种现有法律可能适用于人工智能使用的某些方面。监管方法倾向于渐进式,重点是自愿遵守而非强制性规定。此种方式允许在技术发展和组织适应人工智能带来的新挑战时保持必要的灵活性。

(五)沙特阿拉伯人工智能伦理原则与应用指南

沙特阿拉伯在人工智能治理方面主要依赖于指导原则和现有法律框架,而非专门的人工智能法规。沙特数据和人工智能管理局(Saudi Data and Artificial Intelligence Authority, SDAIA)在这一进程中发挥了关键作用,制定了《人工智能伦理原则》(AI Ethics Principles)和《生成式人工智能的指南草案》(Guide on Generative Artificial Intelligence and Large Language Model)。这些文件虽不具有法律约束力,但为人工智能技术的负责任开发和使用提供了重要指导。《人工智能伦理原则》强调了公平、隐私、可靠性和问责等核心价值,而生成式人工智能指南则为政府雇员和公众使用人工智能技术提供了具体建议,反映了沙特在促进人工智能创新与确保伦理使用之间寻求平衡的方向和意愿。

尽管缺乏专门的人工智能法律,但沙特正在通过其他相关法律框架为人工智能发展创造有利环境。例如,于2024年9月开始执行的《个人数据保护法》(Personal Data Protection Law, PDPL)将对人工智能的开发和使用产生重要影响,特别是在数据隐私和安全方面。此外,作为2030愿景计划的一部分,沙特政府正积极努力建立更为结构化的人工智能监管环境,旨在将国家定位为人工智能和数据驱动经济的领导者。这表明,沙特认识到了人工智能技术的变革潜力,同时也意识到了建立适当监管框架的必要性。



第二篇 人工智能产品出海合规要点分析

随着人工智能技术在全球范围内的迅速发展和广泛应用,企业在国际市场推广和部署人工智能产品的过程中,不仅面临着前所未有的机遇,更面临着日益复杂的监管挑战。这些挑战不再局限于传统的数据隐私保护领域,而是延伸到了算法公平、模型透明度、伦理考量等新兴议题,构成了一个多维度、跨学科的合规难题。鉴于此,本文将聚焦人工智能产品生命周期中的两个关键阶段——大模型训练与开发、产品运营。通过系统梳理这些阶段中可能遇到的法律风险和监管要求,本文将深入分析人工智能产品出海过程中的合规要点,旨在为企业制定全面而有效的合规策略提供切实可行的指导,助力其在全球人工智能市场的激烈竞争中稳步前行和实现可持续发展。

一、大模型训练与开发阶段的合规要求及企业应对

(一)不同跨境数据获取方式的合规性考量

在人工智能大模型的训练与开发过程中,获取高质量、多样化的数据集至关重要,而跨境数据的获取更是为模型的全球适用性提供了关键支撑。然而,面对各国日益严格的数据保护法规和数据主权要求,企业在获取和使用境外数据时需要谨慎行事,权衡效率与合规。通常,企业可以通过以下几种主要方式获取跨境数据:从境外数据经纪人购买、从境外网站爬取数据、利用境外开源网站的数据集,以及直接从境外用户收集数据。上述方法各有特点,也面临着不同的法律风险和合规挑战。

1.从境外数据经纪人购买

企业可以通过数据经纪人从境外合法购买训练数据,其通常包括个人数据、行为数据、市场数据等多种类型,可用于人工智能模型的训练和优化。然而,这种方式存在多重风险,主要涉及隐私与数据保护、数据合法性与来源合规性,以及数据质量与适用性等方面。例如,在处理欧盟公民数据时,企业必须严格遵守《通用数据保护条例》(General Data Protection Regulation, GDPR)的要求,确保数据主体的知情同意、数据最小化、存储限制等原则。违反GDPR可能导致高达2000万欧元或全球年营业额4%(以较高者为准)的罚款。

针对此种数据获取方式,企业应选择声誉良好、具有相关资质的数据经纪人,并应与其签署详细的数据处理协议,明确数据的来源、使用范围和责任划分。与此同时,企业需要进行尽职调查,确保数据的收集和处理符合原始数据所在地的法律要求,以确保购买的数据符合企业的合规标准和质量要求。

2.从境外网站爬取数据

通过爬虫技术从境外网站或平台自动抓取公开数据是一种常见的做法,特别是对于需要大量非结构化数据(如文本、图片和视频)的人工智能模型训练。但这种方式面临着多方面的法律风险,包括违反相关法律法规、侵犯知识产权,以及违反网站使用政策等。在美国,未经授权的数据爬取可能违反《计算机欺诈和滥用法》(Computer Fraud and Abuse Act, CFAA)。虽然2021年的Van Buren v. United States案例在某种程度上限制了CFAA的适用范围,但企业仍需谨慎行事。在欧盟,如果爬取的数据包含个人信息,可能违反GDPR的规定。此外,爬取的数据可能涉及第三方的版权或数据库权利,特别是在欧盟,《数据库指令》(Directive 96/9/EC on the Legal Protection of Databases, Database Directive)为数据库的创建者提供了特殊的法律保护。

为了合规地进行数据爬取,企业应仔细研究目标网站的使用条款和robots.txt文件,尊重网站的爬虫政策。考虑与数据源网站建立正式的数据共享协议也是一个可行的选择,这可以大大降低法律风险。在技术层面,实施措施控制爬取速率,以减少对目标网站的负面影响。对爬取的数据进行严格的筛选和处理也是必要的,确保不包含个人隐私信息或受版权保护的内容。

3.从境外开源网站获取数据

从GitHub、Kaggle等开源平台获取数据集是一种便捷且广泛使用的方式。这些数据通常在开放许可(如MIT、Apache、CC-BY等)的基础上提供给开发者和研究人员使用。然而,使用开源数据仍然存在一些潜在风险,主要涉及开源许可的合规性、隐私风险,以及数据质量和责任问题。不同的开源许可对数据的使用有不同的限制,某些许可可能要求在使用数据的产品中包含原始许可文本,或者限制商业使用。尽管开源数据集通常经过处理,但仍可能包含未经适当匿名化的个人信息,使用这些数据可能无意中违反隐私保护法规。此外,开源数据的质量可能参差不齐,且数据提供者通常不对数据的准确性或合法性负责。

因此,企业需要自行承担使用这些数据带来的风险。为了安全合规地使用开源数据,企业可以建立专门的开源合规团队,负责审核和管理所使用的开源数据集,并创建开源数据使用清单,详细记录每个数据集的来源、许可类型和使用范围。这可以帮助企业更好地管理合规风险。

4.直接从境外用户收集数据

直接从境外用户收集数据可以获得高质量、定制化的训练语料,但也面临着最复杂的隐私保护法规挑战。这些挑战主要涉及隐私与数据保护法律、跨境数据传输,以及数据安全等方面。不同国家和地区的数据保护法规要求各不相同,例如,GDPR要求企业必须有明确的法律基础来处理个人数据,并赋予用户多项权利,如访问权、删除权、数据可携带权等。在美国,除了联邦法律,还需要考虑各州的隐私法规,如《加州消费者隐私法案》(California Consumer Privacy Act, CCPA)和《弗吉尼亚消费者数据保护法》(Virginia Consumer Data Protection Act, VCDPA)。许多国家对个人数据的跨境传输有严格限制,例如,GDPR要求将数据传输到欧盟以外的国家时,必须确保该国具有“充分的数据保护水平”,或采取适当的保障措施,如标准合同条款(SCCs)。此外,跨境收集和传输数据增加了数据泄露的风险,一旦发生数据泄露,企业可能面临多个司法管辖区的处罚和诉讼。

为此,企业需要制定全面的隐私政策,清晰说明数据收集的目的、使用方式和用户权利,实施用户同意管理系统,确保获得用户的明确同意,并允许用户随时撤回同意。在欧盟等地区,采用隐私设计(Privacy by Design)原则,在产品设计初期就考虑隐私保护,可以大大降低后期的合规风险。在成本允许的情况下,考虑在不同地区部署本地化的数据中心,以满足数据本地化要求,也是一种有效的合规策略。

(二)大模型开源的合规性考量

1.模型开源的阶段划分

人工智能系统的开源与传统软件开源存在显著差异。人工智能系统由多个组成部分构成,包括推理代码、训练代码、模型权重和训练数据。这种复杂性使得人工智能系统的开源程度可以划分为多个层次,从完全开放到完全封闭,形成了一个连续的谱系。目前,业界普遍将人工智能系统的开放程度划分为七个不同的级别:

(1)完全开放:代码(包括推理代码和训练代码)、模型权重和训练数据均对外开放且无使用限制。例如,EleutherAI的GPT-NeoX模型就采用了这种完全开放的方式。

(2)开放但有限制:代码、模型权重和训练数据均对外开放,但附带一定的使用限制。BigScience的BLOOM模型就属于这一类型。

(3)仅开放模型权重:只公开模型权重,而不公开代码和训练数据。Stability AI的Stable Diffusion模型和Meta的Llama 2模型采用了这种策略。

(4)API开放且可微调:通过API提供模型服务,并允许用户进行微调。OpenAI的GPT-3.5模型就采用了这种方式。

(5)API开放但不可微调:通过API提供模型服务,但不允许用户进行微调。OpenAI的GPT-4模型属于这一类型。

(6)网页访问:仅通过网站页面提供模型服务。Inflection AI的Pi模型就采用了这种方式。

(7)完全封闭:除开发人员外,外部人员无法获取或使用模型。Google DeepMind的Flamingo模型属于这一类型。

近年来,各国政府开始关注并制定针对人工智能模型开源的相关法规,反映了促进技术创新的愿望,也体现了对国家安全和公共利益的考量。

在美国,2024年5月8日,美国众议院外交事务委员会和两党议员提出了法案(H.R.8315-Enhancing National Frameworks for Overseas Restriction of Critical Exports Act)。该法案旨在修订2018年《出口管制改革法案》,赋予政府更大的权力来管控人工智能模型的出口。这一举措反映了美国政府对人工智能技术国家安全影响的关注,可能会对人工智能模型的国际合作和开源产生重大影响。

欧盟在《人工智能法案》中对人工智能系统的开源提供了更为详细的规定。该法案在第2条明确了适用范围,对免费且开源的人工智能系统给予了一定的豁免。但这种豁免并非无限制的,主要存在以下几个例外情况:

(1)高风险人工智能系统:即使是开源的高风险人工智能系统,仍需遵守透明度、数据质

量、记录保存、人工监督和稳健性等要求。

(2)不可接受风险类人工智能系统:对于可能造成重大伤害或侵犯基本权利的人工智能系统,无论是否开源,都被明令禁止。

(3)通用人工智能模型:对于具有系统风险的通用人工智能模型(如训练计算量超过10²⁵ FLOPs),即使开源也需遵守相关规定。其他通用人工智能模型则需遵守版权法和信息披露要求。

(4)特定类型人工智能系统:直接与人类互动的人工智能系统,即使开源,也需遵守透明度义务,如告知用户正在与人工智能系统互动,标注人工智能生成的内容等。

2.企业应对策略

面对复杂的人工智能开源环境和不断演变的法规要求,企业在开源人工智能模型时需要采取全面的合规策略。首先,企业应建立完善的开源评估机制,考虑技术、法律、商业和伦理等多个因素,以决定是否开源及采取何种开源级别。其次,在开源前进行全面的合规性审查,确保模型不属于法规禁止的高风险或不可接受风险类别。同时,企业需要明确定义开源范围,选择合适的开源许可,并提供详细的技术文档,包括模型的功能、局限性和潜在风险。此外,企业还应建立持续监控机制,密切关注法规变化和模型使用情况,及时调整开源策略。最后,对于跨国经营的企业,需特别注意不同国家和地区的法规差异,在进行国际合作或向海外开源时,充分考虑可能的出口管制和数据跨境传输限制。通过这些措施,企业可以在推动人工智能技术创新和开放共享的同时,有效管理法律风险,确保合规经营。

(三)满足多国人工智能伦理标准的研发实践

2023年11月1日,在英国布莱切利园召开的全球首届人工智能安全峰会上发布的《布莱切利宣言》(The Bletchley Declaration),为我们提供了一个理解国际社会对人工智能安全和伦理要求的重要窗口。这份宣言汇聚了来自中国、美国、欧盟等28个国家的政府代表,以及全球学术、科研机构 and 知名企业的共识,反映了当前国际社会对人工智能发展的普遍关切。宣言强调了以人为本的人工智能开发理念,呼吁在设计、开发和使用人工智能时,确保其安全、值得信赖和负责任。对于计划进行国际化发展的人工智能企业来说,深入理解并遵循这些国际普遍认同的人工智能安全要求至关重要。

《布莱切利宣言》指出,人工智能技术不仅为全球带来了巨大的发展机遇,还在医疗、交通、教育等多个领域深刻影响着人们的日常生活。然而,伴随这些机遇而来的风险和挑战同样不容忽视。宣言特别提到了前沿人工智能技术(如通用人工智能模型)可能带来的潜在风险,包括滥用或失控问题。通过关注这些国际普遍认同的人工智能安全要求,企业不仅可以更好地满足多国的监管标准,还能增强其产品在全球市场的竞争力和可信度。

在全球范围内,各国政府正在积极制定针对人工智能的具体规范和底线要求。这些要求虽然在细节上有所不同,但都体现了对人类尊严、自由、平等、隐私等基本价值的共同关注。例如,美国政府要求开发潜在双重用途基础模型的公司向联邦政府提供相关信息,包括训练过程的安全措施、模型权重的保护措施以及红队测试结果等,反映了美国政府对人工智能安全性和潜在风险的高度重视,尤其是在国家安全和关键基础设施保护方面。欧盟的《人工智

能法案》则更加详细地列举了被禁止的人工智能实践,包括潜意识操纵、利用人的弱点、社会评分、预测犯罪倾向等。这些禁令体现了欧盟对人的尊严、自由、平等、民主和法治等价值观的坚持,以及对个人隐私和数据保护的重视。特别是,欧盟明确禁止利用人工智能系统对个人进行不合理的评分或歧视性对待,反映了其对社会公平和个人权利的强调。

对于计划出海的人工智能企业来说,遵守多国的伦理标准既是挑战也是机遇。面对全球范围内日益严格的人工智能伦理要求,企业在研发实践中需采取全面而灵活的应对策略,以确保其人工智能产品不仅技术先进,更符合国际普遍认可的伦理标准。首要之务是建立健全的伦理审查机制,该机制应贯穿产品设计、开发和应用的全过程,确保每个阶段都充分考虑并遵循各目标市场的伦理要求,尤其要关注《布莱切利宣言》中强调的以人为本、安全可靠和负责任的开发理念。其次,企业应着力培养跨学科的人工智能伦理专家团队,该团队不仅精通技术开发,还应深谙各国的法律法规和文化背景,能够准确把握不同地区对人工智能伦理的特定要求,从而在产品开发中预见并避免潜在的伦理风险。

此外,企业还应建立完善的风险评估体系,特别是针对前沿人工智能技术(如通用人工智能模型)可能带来的潜在风险,进行全面而深入的评估,包括但不限于滥用风险、失控风险以及对社会公平和个人权利的潜在影响。通过定期的“红队”测试和伦理影响评估,不断优化产品设计和功能,以最大程度地降低伦理风险。同时,企业应当建立透明的信息披露机制,主动公开其人工智能系统的基本原理、数据来源和潜在影响,特别是在涉及个人隐私、社会公平和国家安全等敏感领域时,更应采取额外措施确保信息的透明度和可解释性。

最后,企业应积极参与国际人工智能伦理标准的制定过程,通过与政府机构、学术界和其他行业参与者的密切合作,共同推动形成更加统一和可操作的全球人工智能伦理框架,为国际标准贡献智慧的同时,也能更好地预见和适应未来的监管趋势,从而在激烈的全球竞争中赢得先机和主动。

二、人工智能产品运营方式的合规要求及企业应对

(一)人工智能C端应用

1.人工智能C端应用的合规要求

人工智能C端应用的合规性是一个多层面的挑战,涉及数据隐私、水印标识、内容审核等多个关键领域。对于计划出海的人工智能企业来说,需要特别关注几个方面,尤其是快速变化的法律环境。最近,加州 AB-3211 法案(California Digital Content Provenance Standards)的提出就是一个典型例子,该法案得到了 OpenAI、微软和 Adobe 等科技巨头的支持,要求在加州标记人工智能生成的内容。这一趋势表明,内容标识和溯源将成为人工智能应用,特别是生成式人工智能应用的重要合规要求。该法案要求文生图模型必须嵌入详细、不可见且难以移除的元数据,以便识别人工智能生成的图像,并提供生成方式、时间等信息。这不仅增加了技术难度,还可能带来额外的法律风险。

在开发人工智能C端产品时,企业还需要特别关注生成内容的知识产权问题。2023年

12月,《纽约时报》对OpenAI及其投资人提起诉讼,指控ChatGPT侵犯版权,这一案例凸显了人工智能生成内容面临的法律风险。诉讼指出,ChatGPT在构建数据库、深度学习过程中未经许可使用《纽约时报》的内容,有时甚至一字不差地复制或伪造新闻报道。这种情况不仅涉及版权侵犯,还可能导致虚假信息传播。为了缓解这种风险,人工智能企业在开发C端产品时应采取多重措施:首先,在训练数据选择上要更加谨慎,确保有合法的使用权;其次,在模型训练过程中应实施严格的数据处理和过滤机制,避免直接复制版权内容;再者,在内容生成环节,可以采用机器审核或人工审核相结合的方式,识别和过滤可能存在版权问题的内容。此外,企业还应建立完善的用户反馈机制,及时处理可能的侵权投诉。

2.企业应对策略

企业还需要高度重视生成内容的内容合规性问题,以降低潜在的法律和声誉风险。以2024年8月xAI发布的Grok 2大模型为例,其能够精确生成和融合名人肖像,导致社交平台上出现大量“虚假图片”,引发了广泛的社会关注和争议。这种深度伪造技术的进步虽然展示了人工智能的强大能力,但同时也带来了严重的伦理和法律挑战。对人工智能企业而言,如何防止其技术被滥用于制作虚假或误导性内容,成了一个亟须解决的问题。为此,企业应采取多项措施:首先,在产品的设计阶段就应考虑内容审核机制,如实施强有力的身份验证和使用授权系统,限制敏感功能的使用范围。其次,可以开发和部署先进的内容检测算法,自动识别和标记可能的深度伪造内容。再者,建立用户举报和快速响应机制,及时处理可能违规的内容。

(二)向域外提供调用API服务的合规

1.向域外提供调用API服务的合规要求

向域外提供调用API服务是人工智能企业国际化发展的重要方式之一。API(应用程序接口)可以理解为不同软件系统之间的“翻译官”,其定义了一套规则,使得不同的软件能够相互交流和交换信息。当人工智能企业向域外客户提供API调用服务时,实际上是在搭建一座数字桥梁,让国外客户的软件能够与企业的人工智能系统进行无缝对接和交互。

这一过程通常包含三个关键步骤:首先,域外客户的软件(客户端)向人工智能企业的API发送请求,就像是在询问一个问题;其次,人工智能企业的系统接收到这个请求后,会进行分析和处理,这相当于根据问题查找答案;最后,处理完成后,系统会将结果通过API返回给客户端,完成整个交互过程。在这个过程中,数据的流通是核心。数据首先通过互联网在客户端和人工智能企业的服务器之间传输。为了确保安全,这些数据在传输过程中通常会进行加密,就像将重要文件放入保险箱中传递。当数据到达人工智能企业的服务器后,服务器会根据接收到的请求提供相应的服务或数据,然后再将结果通过网络安全地返回给客户。

在向域外提供调用API服务时,企业需要确保数据存储和处理符合客户所在国的法律要求。这不仅涉及数据隐私保护,还包括遵守各国的数据本地化要求和跨境数据传输规定。例如,欧盟的GDPR对个人数据的处理和传输有严格的规定,而俄罗斯等国家则要求个人信息等数据必须存储在本国境内服务器上。因此,人工智能企业需要深入了解目标市场的相关法规,并据此调整其数据处理和存储策略。

云服务厂商的选择也是一个关键考量。特别是在面对像美国这样实施严格出口管制的国家时,选择合适的云服务提供商变得尤为重要。以美国2023年发布的《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》(Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern)为例,该命令旨在限制美国人参与某些国家的相关数据交易。这意味着,如果人工智能企业涉及处理大量美国敏感个人数据,或者从事数据中介业务,就可能受到该命令的限制。

2.企业应对策略

为了降低合规风险,人工智能企业可以采取以下策略:

1. 尽量减少收集和处理敏感个人数据,特别是来自受限制国家的数据。
2. 避免直接与受限制国家的实体进行数据中介活动。
3. 考虑与非受关注国家的实体合作处理国际客户数据。
4. 选择在目标市场拥有数据中心的云服务提供商,以满足数据本地化要求。
5. 实施严格的数据分类和访问控制机制,确保敏感数据的安全。

通过实施这些策略,人工智能企业可以在国际化发展过程中更好地管理合规风险,建立起强大的数据保护机制,从而赢得客户信任,实现可持续的全球化发展。

(三)域外私有化部署的合规

1.域外私有化部署的合规要求

域外私有化部署是人工智能企业国际化的另一种重要方式,它涉及将人工智能系统直接部署在客户的本地环境或指定的私有云中,以能够更好地满足某些行业或地区对数据主权和安全的严格要求,但同时也带来了独特的合规挑战。域外私有化部署作为人工智能企业国际化的一种方式,相较于直接提供C端产品或API服务,在合规方面具有显著优势。一方面,私有化部署能够更好地满足数据本地化要求。通过私有化部署,企业可以确保所有数据处理和存储都在客户的本地环境中进行,从而有效规避跨境数据传输的合规风险。另一方面,私有化部署有助于降低数据泄露风险。与C端产品或API服务可能面临的大规模数据泄露不同,私有化部署将数据控制权完全交给客户,大大减少了企业在数据保护方面的责任和风险,这对于处理敏感数据的行业,如金融、医疗等行业,尤其重要。

然而,选择私有化部署也面临着一些挑战。首先是技术出口管制的问题。以美国为例,其《出口管制条例》(Export Administration Regulations,EAR)对某些高级技术的出口有严格限制。人工智能企业在进行域外私有化部署时,需要仔细评估其技术是否属于受管制范围,并在必要时申请相应的出口许可。另一方面,一些国家可能会实施技术本地化政策,要求关键技术必须由本地企业提供或掌握。华为在全球5G市场遭遇的阻力就是一个典型例子。为应对这种挑战,人工智能企业可能需要考虑与当地企业合作,进行技术转让或合资经营,以满足本地化要求。

2.企业应对策略

针对域外私有化部署的合规挑战,企业可采取以下策略:首先,建立专门的国际合规团

队,深入研究目标市场的技术出口管制和数据本地化要求,制定符合当地法规的部署方案。其次,考虑采用模块化设计,将核心技术与本地化模块分离,既保护知识产权,又满足合规需求。此外,积极寻求与当地企业的战略合作,通过合资或技术授权等方式,既遵守本地化政策,又降低市场准入门槛。最后,建立灵活的风险评估机制,定期审查各国法规变化,及时调整部署策略,确保长期合规经营。通过上述措施,企业可在保障合规的同时,充分发挥私有化部署的优势,实现全球业务的稳健发展

三、人工智能产品部署阶段的合规要求及企业应对

(一)部署后的模型安全保障

1.合规要求

在人工智能产品部署后的阶段,确保模型的安全性不仅关乎企业的商业利益,更涉及用户隐私和社会安全,成为企业面临的首要挑战和监管机构关注的重点。模型安全保障主要涵盖算法安全、网络安全和模型安全三个方面,每个方面都有其特定的合规要求和潜在风险。在算法安全领域,防范模型参数中的信息被窃取成为核心任务,包括抵御提示词攻击和各种算法攻击,以确保模型的核心知识产权得到有效保护;而在网络安全方面,如2019年Capital One遭遇的数据泄露事件所警示的那样,配置错误或安全漏洞可能导致大规模用户敏感信息泄露,因此,强化网络安全措施成为不可或缺的合规要求;至于模型安全,则主要聚焦于防止人工智能系统被滥用于非法或有害目的,特别是那些可能导致严重后果的情况,如利用人工智能系统制造大型生物武器等,这要求企业建立全面的安全评估和防护机制。

2.企业应对策略

面对上述复杂而严峻的安全挑战,人工智能企业需采取全面而系统的应对策略。在算法安全方面,企业应实施严格的访问控制机制,采用先进的加密技术保护模型参数,并建立定期更新和优化防御策略的机制,以应对不断演变的攻击手段;在网络安全领域,企业应构建多层防护体系,包括但不限于定期进行全面的安全审计、部署先进的入侵检测和防御系统、加强员工安全意识培训,以及建立快速响应机制以应对可能发生的安全事件,从而在技术和管理两个层面筑起坚实的安全防线;对于模型安全,企业应组织专业的“红队”,定期进行全面而深入的安全测试,模拟各种可能的攻击场景,特别关注那些可能导致严重后果的情况,通过这些测试不断识别并修复潜在的安全漏洞,确保模型在各种极端情况下都能保持安全和可控。此外,企业还应建立跨部门的安全响应团队,制定详细的应急预案,并定期进行演练,以确保在实际遇到安全威胁时能够迅速、有效地做出反应,从而最大限度地降低潜在损失和影响。

(二)用户数据的保护与合规利用

1.合规要求

在人工智能技术日新月异的背景下,用户数据的保护与合规利用已成为企业面临的重大挑战,2024年9月爱尔兰数据保护委员会(DPC)与X公司(前Twitter)就使用欧盟公民个人

数据训练人工智能聊天机器人 Grok 的法律诉讼和解案例,为行业提供了深刻启示,凸显了几项关键的合规要求:首先,用户明确同意原则成为数据收集和使用的基石,特别是在涉及人工智能模型训练等新兴技术应用时,企业必须清晰说明数据用途并获得用户的明确授权,确保用户充分理解并同意其数据的使用方式;其次,数据最小化原则在人工智能时代愈发重要,企业在追求大数据和模型性能的同时,必须谨慎评估每一类数据的必要性,仅收集和处理完成特定目的所必需的数据,避免过度收集导致的合规风险和用户信任损失;最后,跨境数据保护合规成为全球化背景下的新挑战,企业必须同时应对多个司法管辖区的数据保护要求,这要求建立全面的国际合规体系,密切关注各地区的数据保护法规变化,并能够灵活调整数据策略以适应不同市场的监管环境。

2.企业应对策略

首先,在数据收集环节,企业应建立健全的用户同意管理机制,设计清晰、易懂的数据使用说明和隐私政策,采用分层同意等创新方式,确保用户在充分理解的基础上做出选择,同时,针对人工智能模型训练等特殊用途,可考虑设立专门的知情同意程序,进一步强化用户权益保护;其次,在数据处理方面,企业应实施严格的数据最小化战略,建立数据分类分级制度,定期评估数据收集的必要性和合理性,并通过技术手段(如数据脱敏、匿名化处理)降低不必要的数据收集和存储,同时,建立定期数据审查和清理机制,确保长期合规;最后,针对跨境数据合规挑战,企业应组建专业的国际合规团队,深入研究各目标市场的数据保护法规,制定灵活的数据本地化策略,如在不同地区部署独立的数据中心,或采用联邦学习等先进技术实现跨境数据协作而不直接传输原始数据,此外,企业应积极参与国际数据保护标准的制定和行业自律,通过与各国监管机构、行业协会的沟通与合作,不仅能更好地预见和适应未来的监管趋势,还能在塑造合理、可行的国际数据保护框架中发挥积极作用。

(三)人工智能产品的可解释性与透明度要求

1.合规要求

在人工智能产品的部署阶段,可解释性与透明度已然成为监管机构和行业标准制定者关注的焦点,不仅体现在法规要求上,更反映在技术标准的制定中,两者共同构筑了人工智能产品合规的重要支柱,为企业设定了明确而严格的指导方针。从法规角度观之,欧盟《人工智能法案》(AI Act)第49条对人工智能系统的登记提出了明确要求,该要求不仅涵盖了高风险人工智能系统,更延伸至某些非高风险系统,充分体现了监管机构对人工智能产品透明度的高度重视,具体而言,法案要求人工智能系统提供者或授权代表在将系统投放市场或提供服务之前,必须在欧盟数据库中进行登记,登记内容涵盖系统的基本信息、性能特征以及使用情况等,此举旨在增强人工智能系统的可追溯性和公众监督。同时,对于涉及执法、移民和边境管控等敏感领域的高风险人工智能系统,法案还特别规定了更为严格的登记要求,包括在数据库的非公开部分进行登记,并限制访问权限,前述规定充分体现了在保障透明度的同时,也需要兼顾数据安全和隐私保护的平衡之道。

从行业标准的视角审视,欧洲电信标准协会(ETSI)发布的一系列报告,尤其是ETSI GR SAI 007 报告(Explicability and Transparency of AI Processing),为人工智能系统的可解释

性和透明度提供了详尽的技术指导。该报告将可解释性分为静态和动态两种形式,其中静态可解释性强调系统文档的编写,要求非专业人士也能理解系统的目的、数据来源和处理过程,而动态可解释性则聚焦于系统运行时的行为解释,确保开发者和利益相关者能够实时了解系统决策的依据。此外,ETSI还提出了基于XAI(可解释人工智能)技术的应用方法,包括概率方法和逐层相关性传播(LRP)等技术,上述方法有助于深入剖析人工智能模型的行为和决策过程,特别是在复杂的预测任务中,能够有效提升系统的可解释性。值得一提的是,ETSI的报告还特别强调了数据透明度的重要性,指出数据完整性检查是透明度的核心,要求确保数据在传输过程中不被篡改,同时对数据的来源、真实性和共享权限进行严格验证,前述措施不仅能提高人工智能系统的透明度,更能确保系统在处理数据时符合安全和合规要求。

2.企业应对策略

面对上述严格而全面的可解释性与透明度要求,人工智能企业需采取系统化、多层次的应对策略。首先,在系统设计阶段,企业应将可解释性作为核心设计原则之一,采用先进的可解释人工智能技术,如LIME(Local Interpretable Model-agnostic Explanations)或SHAP(SHapley Additive exPlanations)等方法,构建能够提供清晰决策路径和依据的模型架构。同时,企业还应建立完善的文档体系,包括但不限于系统架构说明、数据处理流程、决策逻辑等,确保即便是非技术背景的利益相关者也能理解系统的基本运作原理。

其次,在系统部署和运营阶段,企业应建立健全的透明度管理机制,包括定期发布系统性能报告、主动披露重大算法更新、设立用户查询和反馈渠道等,通过这些措施,不仅能够满足监管要求,更能增强用户和公众对人工智能系统的信任。此外,对于涉及敏感领域的高风险系统,企业应考虑建立独立的第三方审核机制,邀请外部专家定期评估系统的公平性、安全性和合规性,并公开审核结果,以进一步提高系统的透明度和可信度。

最后,在数据管理方面,企业应实施严格的数据治理策略,包括建立数据溯源机制、实施数据完整性检查、制定详细的数据共享和访问控制政策等,通过这些措施,不仅能确保数据的透明度和可信度,还能有效防范数据篡改和滥用风险。同时,企业还应积极参与行业标准的制定和最佳实践的分享,通过与监管机构、学术界和同行的深入交流与合作,不断完善自身的可解释性和透明度实践,在推动行业发展的同时,也能在日益严格的监管环境中保持竞争优势。

(四)人工智能产品责任分析

1.欧盟《人工智能法案》中的主体划分

欧盟《人工智能法案》针对人工智能产品的责任主体进行了细致的划分,主要包括提供者(Provider)、部署者(User)以及进口商和分销商(Importer and Distributor)三类。这种划分明确了供应链各环节的具体责任,有助于全面管理人工智能系统的风险。

2.不同主体的责任分析

提供者作为人工智能系统的开发者,承担着最为广泛和严格的责任。根据第16条和第17条,提供者需要确保系统合规、进行标识、建立质量管理体系、保留文件等。第43条要求提供者在产品投放市场前进行严格的合规评估,第72条则规定了建立上市后监控机制的要求。

部署者虽然不直接参与系统的开发,但在实际使用过程中扮演着关键角色。第26条详细列举了部署者的主要义务,包括按照使用说明使用系统、指派合格人员进行监督、监测系统运行等。第27条还要求部署者进行基本权利影响评估,以确保系统的使用不会侵犯个人权益。

进口商和分销商作为供应链的重要环节,也承担着相应的责任。根据第23条和第24条,他们需要在产品进入市场前核实提供者的合规性和产品的合格性认证,确保产品上标明必要的信息,并在必要时协助监管机构的工作。

3.人工智能产品责任的特点与发展趋势

《人工智能法案》的责任划分体现了人工智能产品责任的复杂性和全面性。首先,责任主体的多元化要求供应链各环节都需要承担相应的法律义务,这增加了合规的难度。其次,法案强调了全生命周期的风险管理,从产品开发、投放市场到后续监控都有严格要求。最后,法案特别关注高风险人工智能系统,对这类系统提出了更高的合规标准。

从《人工智能法案》的规定可以看出,人工智能产品责任的发展呈现出以下趋势:第一,责任主体的细化。法案不再简单地将责任划分给开发者和使用者,而是根据供应链的不同环节细化责任主体,这种趋势可能会在未来的立法中进一步发展。第二,全生命周期管理。法案要求从产品开发到市场监控的全过程都要进行风险管理,这种全面性的要求可能会成为未来人工智能产品责任的标准。第三,差异化管理。法案对高风险人工智能系统提出了更严格的要求,这种根据风险程度进行差异化管理的方式,可能会在未来的立法中得到更广泛地应用。

4.对中国企业的启示

首先,中国企业在进入欧盟市场时需要准确识别自身角色,明确是提供者、部署者还是进口商/分销商,以准确把握相应的法律义务。其次,企业应全面履行合规义务,特别是对于高风险人工智能系统,需要建立完善的质量和风险管理体系。最后,企业需要加强法律和伦理意识,密切关注欧盟法规的更新,并将伦理考量纳入产品设计和运营的全过程。



第三篇 人工智能产品出海的文化适应与未成年人保护

人工智能技术正以前所未有的速度重塑全球产业格局和社会生活。根据《2023 全球人工智能创新指数报告》，2023 年全球机器学习模型数量同比增长 91.2%，创下近十年最大增幅。产业界在模型开发上的优势日益突出，独立研发的机器学习模型数量达到学术界的 3.5 倍。特别是在生成式人工智能领域，开源项目数量从 2022 年的 1.7 万个激增至 2023 年的 6 万个，充分体现了这一领域的蓬勃发展势头。

然而，随着人工智能技术的快速发展和广泛应用，其所带来的文化冲击和对未成年人的潜在影响也日益凸显。在全球化背景下，人工智能产品面临着如何适应不同文化背景、价值观念和监管环境的挑战。同时，如何在推动创新的同时保护未成年人的权益，成为各国政府、企业和社会各界共同关注的重要议题。

本文将深入探讨人工智能产品在全球化进程中的文化适应策略，以及在未成年人保护方面的合规要点。通过分析主要市场的文化特征、价值观差异及其对合规策略的影响，为企业提供切实可行的本地化设计和内容审核机制建议。同时，文章将重点阐述人工智能产品对未成年人的潜在影响，并就如何设计和实施有效的保护机制提供指导。

一、全球化背景下的人工智能产品的文化适应

(一)主要市场的文化特征及价值观差异

1. 欧盟：关注数据隐私与算法透明度要求

欧盟在应对人工智能带来的文化与伦理挑战时，深深植根于其独特的历史背景和价值观体系。欧洲文化长期以来就高度重视个人权利、隐私保护和社会公平，这些价值观在数字时代面临新的挑战 and 诠释。特别是在经历了 20 世纪的极权主义后，欧洲社会对个人隐私和数据保护格外敏感。同时，欧洲的民主传统也要求在新技术应用中保持透明度和可问责性，以维护公民权益和社会信任。

基于这些文化和伦理考量，欧盟制定了一系列旨在规范人工智能发展的法律法规。《通用数据保护条例》(General Data Protection Regulation, GDPR)就是对欧洲隐私文化的法律化体现，它赋予了个人对自身数据的控制权。《人工智能法案》则进一步反映了欧洲对人工智能伦理的思考，特别是在算法透明度和公平性方面。这部法案不仅关注技术标准，更试图将欧洲的人文关怀融入人工智能发展中，确保人工智能系统的决策过程可追溯、可解释，并符合欧洲的伦理标准。

上述法规的实际应用进一步凸显了欧盟在文化和伦理方面的关切。2023 年 3 月，意大利

暂停 ChatGPT 服务的决定,不仅是对 GDPR 的执行,更反映了欧洲社会对人工智能可能侵犯个人隐私和自主权的深层忧虑。同样,2024 年 9 月荷兰对 Clearview AI 的巨额罚款,体现了欧洲在面对新兴技术时,如何权衡社会安全与个人隐私的伦理困境。这一决定彰显了欧洲在人脸识别等敏感技术应用上的谨慎态度,以及对防止大规模监控社会出现的决心。

在算法透明度方面,2024 年 3 月法国对谷歌的处罚不仅涉及技术合规问题,还触及了更广泛的文化和伦理议题。这一案例反映了欧洲如何在数字时代保护其丰富的文化遗产和知识产权,同时也体现了对人工智能系统在内容创作和传播中角色的伦理思考。《数字服务法案》(Digital Services Act, DSA)和《数字市场法案》(Digital Markets Act, DMA)中要求大型平台定期发布透明度报告的规定,则是欧洲民主传统在数字领域的延伸,旨在确保公众对影响深远的人工智能系统有知情权和监督权。

2.美国:考虑性别、种族和政治倾向等多元化因素

美国作为一个多元文化的社会,在应对人工智能产品带来的文化与伦理挑战时,特别关注性别、种族和政治倾向等多元化因素。这种关注源于美国的历史背景、社会结构和当前的政治气候,反映了美国社会对平等、包容和多样性的追求。

在美国,人工智能产品的开发和应用必须考虑到社会的多元化特征。这不仅是法律和管理的要求,更是社会期望的体现。近期谷歌公司的 Gemini 人工智能模型引发的争议就是一个典型案例。Gemini 在生成历史人物图像时,出现了将白人历史人物错误地描绘为有色人种的情况,引发了广泛的讨论和批评。

美国的文化敏感性体现在多个方面:

种族敏感性: 人工智能系统必须避免产生可能被视为种族主义、仇恨言论或强化负面种族刻板印象的内容。Gemini 案例表明,即使是试图增加多样性的努力,如果处理不当,也可能引发争议。

性别与性别认同: 涉及性别认同、性取向或性别表达的内容需要特别谨慎。美国社会对 LGBTQ+ 权益的关注度越来越高,人工智能系统必须避免产生歧视性或不敏感的内容。

政治内容: 鉴于美国当前高度两极化的政治环境,人工智能系统在处理政治相关内容时需要保持中立和客观。避免产生可能被视为政治偏见或煽动性的内容至关重要。

宗教敏感性: 尽管宗教自由在美国受到强力保护,但人工智能系统仍需谨慎处理涉及宗教的内容,以避免冒犯或攻击特定宗教群体。

在法律框架方面,美国虽然强调言论自由,但仍有一些限制。第一修正案保护言论自由,但不包括淫秽内容、诽谤和煽动暴力。人工智能系统需要在这个框架内运作,避免产生可能触犯法律的内容。同时,《通信规范法》(Communications Decency Act, CDA)第 230 条为互联网平台提供了一定的保护,但这并不意味着可以完全放任有害或非法内容的传播。

对于拟出海美国的人工智能企业来说,了解并尊重美国的多元文化背景,建立健全的内容审核机制,对于成功运营至关重要。这不仅涉及技术层面的调整,更需要深入理解美国社会的文化动态和敏感话题。通过谨慎处理种族、性别、政治和宗教等敏感议题,人工智能系统可以更好地服务于多元化的美国社会,同时避免潜在的争议和法律风险。

3.沙特阿拉伯:注重宗教与传统价值观考量

沙特阿拉伯在应对人工智能产品带来的文化与伦理挑战时,主要注重宗教与传统价值观的考量。这种态度深深根植于沙特作为伊斯兰教圣地的独特地位和其保守的社会文化背景。沙特的监管方式反映了其在保护传统价值观和宗教信仰的同时,如何应对现代技术带来的挑战。

在沙特,伊斯兰教义和传统价值观是社会生活和法律制度的基础。这种文化背景直接影响了沙特对互联网内容,特别是人工智能产品的监管态度。沙特政府通过多个机构,如通信和信息技术委员会(Communications and Information Technology Commission, CITC)和视听媒体委员会(General Commission for Audiovisual Media, GCAM),对互联网内容实施严格的审查和控制。这种监管不仅仅是技术层面的,更是对伊斯兰教义和传统价值观的维护。例如,禁止"不道德"内容(如色情或支持LGBT权利的内容)和宣传什叶派意识形态的网站。

沙特的内容合规要求清晰地体现了其文化和伦理关切:首先,禁止在商业促销活动中使用国旗,体现了对国家象征的尊重;其次,严格的互联网审查制度,旨在保护公民免受被认为有害的内容影响;最后,对社交媒体广告的严格管控,包括要求非沙特居民持有许可证才能发布广告。

在隐私保护方面,沙特的法规同样体现了其文化特色。例如,禁止滥用摄像设备侵犯私人生活,这不仅是对个人隐私的保护,也反映了沙特社会对个人空间和尊严的重视,特别是在性别分离的社会背景下。这种规定对于人工智能产品,尤其是涉及图像识别或处理的应用,提出了特殊的挑战。

4.东南亚多元文化背景下的人工智能合规策略:新加坡、马来西亚和越南案例分析

在东南亚地区开发和部署人工智能产品时,企业面临着独特而复杂的文化、法律和社会环境挑战。新加坡、马来西亚和越南这三个国家虽然地理位置相近,但在文化传统、宗教信仰和政治制度上存在显著差异,这直接影响了人工智能产品的合规要求和社会接受度。

新加坡作为一个高度发达的多元文化社会,其人工智能监管重点在于维护种族和宗教和谐,同时强调公共道德和政治中立。新加坡的《防止网络虚假信息和操纵法案》(Protection from Online Falsehoods and Manipulation Act, POFMA)对人工智能生成内容的真实性提出了严格要求,企业需要建立健全的内容审核机制,以防止虚假信息的传播。此外,新加坡的多元种族背景要求人工智能系统在处理文化和宗教相关内容时保持高度敏感性,避免引发种族或宗教间的矛盾。

马来西亚的文化环境受伊斯兰教影响深远,这对人工智能产品的内容生成和应用提出了特殊要求。企业必须确保其人工智能系统能够识别并遵守伊斯兰教义和价值观,避免生成或推荐涉及酒精、赌博或不当行为的内容。马来西亚的《煽动法》(Sedition Act 1948)和《通信与多媒体法》(Communications and Multimedia Act 1998, CMA)进一步限制了可能引起种族或宗教敌意的内容,人工智能系统需要具备识别和过滤这类敏感内容的能力。值得注意的是,LGBTQ+相关内容在马来西亚属于高度敏感话题,人工智能产品在处理此类内容时需格外谨慎。

越南人工智能监管重点在于维护国家意识形态、社会稳定和网络安全。越南信息与通信

部(MIC)制定的监管框架对人工智能产品和互联网内容服务提出了严格要求。根据新的《互联网服务和在线信息管理、提供和使用法令草案》(Draft Decree on the Management, Provision, and Use of Internet Services and Online Information),跨境信息提供者必须遵守一系列复杂的合规义务。首先,跨境信息提供者需要建立严格的内容监控机制,能够在3小时内移除紧急违规内容,24小时内移除普通违规内容。这要求人工智能系统具备快速识别和处理潜在敏感或违法内容的能力。其次,数据本地化要求强制跨境信息提供者在越南境内存储用户个人数据,这对跨国企业的数据管理策略提出了挑战。此外,用户验证机制的实施,特别是对16岁以下用户的特殊要求,需要人工智能系统能够准确验证用户年龄和身份信息。值得注意的是,越南禁止跨境提供在线游戏服务,除非在本地设立实体,这限制了游戏相关人工智能应用的跨境部署。

在内容审核方面,人工智能系统需要具备识别和过滤可能危害国家安全或公共秩序内容的能力,并能够及时响应用户投诉。此外,越南对公共道德的保守态度也要求人工智能产品在处理涉及性行为和道德规范的内容时保持高度谨慎。

为了在越南市场合法运营,企业不仅需要获得相关许可和注册,还需要定期向越南信息与通信部(Ministry of Information and Communication of Vietnam, MIC)提交详细的运营和合规报告。这些严格的监管要求对人工智能系统的设计、开发和部署提出了重大挑战,企业需要不断调整其技术和运营策略,以适应越南不断变化的监管环境。

(二)文化与价值观差异对合规策略的影响

文化与价值观的差异直接影响企业在不同市场的合规策略,人工智能产品在出海过程中必须充分考虑这些差异,以避免潜在的法律和声誉风险。以下通过具体例子说明这些差异如何影响合规策略:

1. 欧盟:数据隐私与保护

在欧盟,数据隐私和保护是核心价值观,这直接体现在严格的法律法规中。2024年8月26日,荷兰数据保护局(Autoriteit Persoonsgegevens, AP)对Uber Technologies Inc 和Uber B.V.处以2.9亿欧元的行政罚款,原因是Uber在2021年8月6日至2023年11月27日期间将欧洲个人数据传输到美国,但未能提供《欧盟一般数据保护条例》(GDPR)第五章规定的适当保障措施。这一案例凸显了欧盟对跨境数据传输的严格要求,人工智能企业必须在产品设计和运营中优先考虑数据本地化和严格的数据保护措施。

2. 美国:透明度与问责制

在美国,虽然联邦层面没有统一的数据保护法,但各州正在加强对人工智能的监管。以加利福尼亚州为例,2024年通过的《前沿人工智能模型安全可靠创新法案》(Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, SB-1047)要求大规模人工智能模型的开发者具备"一键关停"能力,并进行第三方审计。这一举措反映了美国市场对人工智能透明度和问责制的重视,企业需要在产品中内置相应的控制和审计机制。

3. 日本:软法治理与和谐共识

日本的人工智能治理方式则体现了其独特的社会文化特征。日本政府倾向于采用"软法

治理"方式,如2021年发布的《人工智能治理报告》(AI Governance in Japan Ver. 1.0)提倡敏捷治理和多方利益对话。日本的人工智能治理理念强调企业自主治理和灵活适应,反映了日本社会对和谐与共识的重视。

4.沙特阿拉伯:宗教与传统价值观

在沙特阿拉伯等中东国家,宗教和传统价值观对人工智能产品的影响尤为明显。沙特数据和人工智能管理局(Saudi Data and Artificial Intelligence Authority, SDAIA)制定的《人工智能伦理原则》(AI Ethics Principles)强调了公平、隐私、可靠性和问责等核心价值,同时也要求人工智能应用符合伊斯兰教义。这意味着企业在开发面向中东市场的人工智能产品时,不仅要考虑技术和法律合规,还需要确保产品功能和内容符合当地的宗教和文化要求。

二、企业应对文化与价值观差异的合规策略

(一)加强人工智能产品的本地化设计

在全球化背景下,人工智能产品的成功很大程度上取决于其对不同市场文化特征和价值观的适应能力。加强本地化设计不仅是满足用户需求的关键,也是确保合规的重要策略。以下从多个角度探讨如何实现人工智能产品的有效本地化:

1.深入理解本地文化和用户需求

成功的本地化设计首先需要对目标市场的文化、习俗和用户偏好有深入理解。以Kompas.ai的案例为例,该公司在为西方快餐品牌和国际化妆品公司进行跨境品牌本地化营销时,采取了针对性的策略。针对中国市场,通过分析中国消费者的口味偏好和饮食习惯,为快餐品牌定制了符合本地口味的新产品配方,并创作了相应的营销内容。这种深度本地化不仅提高了品牌知名度,还增强了消费者忠诚度。针对印度市场,分析了印度消费者的美容观念和产品偏好,为化妆品公司推出了符合印度审美和文化习惯的产品包装和广告宣传,显著提升了品牌在印度市场的表现。

2.灵活应对文化敏感问题和避免文化禁忌

在某些市场,特定的文化或政治因素可能对人工智能产品的内容和功能产生重大影响。例如,在某些国家,可能需要对人工智能生成的内容进行特定的审查,以确保符合当地法律和文化规范。在自然语言处理模型中,考虑到某些地区对特定词汇或表达的敏感性,需要加入相应的筛选和替换机制。此外,根据不同文化的审美偏好和使用习惯,调整产品的视觉设计和交互方式也是必要的。

特别重要的是,企业必须格外注意避免触碰当地的文化禁忌,这可能会导致严重的负面后果。以下是两个具体的例子:

在泰国,王室是一个极其敏感的话题。任何被视为不敬或批评王室的内容都可能触犯严格的冒犯君主罪法律。因此,人工智能产品,特别是内容生成或社交媒体相关的应用,必须在其算法和内容筛选机制中加入相应的保护措施,以避免生成或传播任何可能被视为不敬王室的内容。

在印度,牛被许多人视为神圣动物,特别是在印度教文化中。因此,涉及食品、餐饮或生活方式的人工智能应用在印度市场需要特别谨慎。例如,餐厅推荐系统或食谱生成器应该能够识别并尊重这一文化禁忌,避免向素食者或印度教徒推荐含牛肉的餐厅或食谱。

这种对文化敏感性的高度重视和灵活应对,不仅可以帮助企业避免潜在的文化冲突和法律风险,同时提高产品在当地市场的接受度。

(二)建立多样化且灵活的内容审核机制

在计划出海的人工智能产品中,建立多样化且灵活的内容审核机制不仅是合规的需要,也是尊重不同文化和价值观的体现。企业应当根据目标国家或用户群体的特点,设计和实施能够快速调整的内容审核系统。

以美国市场为例,对"种族、性别多样化与政治相关内容"的敏感度较高。人工智能产品在处理这类内容时,需要特别注意避免潜在的歧视或偏见。例如,在招聘相关的人工智能应用中,系统应能识别并过滤掉可能导致种族或性别歧视的措辞;在新闻聚合或社交媒体内容推荐中,算法应当平衡不同政治观点,避免造成信息茧房。相比之下,在伊斯兰国家,对"猪或其他宗教禁忌相关的内容"的审核尤为重要。例如,在食品相关的人工智能应用中,系统需要能够识别并标记含有猪肉成分的产品,或者在图像识别和生成中避免出现与伊斯兰教义不符的内容。在印度,由于复杂的种姓制度历史和当前的社会敏感性,人工智能系统需要特别注意避免任何可能被解读为种姓歧视的内容。这可能涉及职业推荐、婚恋匹配等多个应用领域。

计划进行出海的企业可以采取多种方法,以建立有效的内容审核机制。首先,可以利用机器学习技术来识别不同文化背景下的敏感内容,并持续更新数据集以适应社会规范的变化。其次,应建立多层级审核系统,结合自动化审核和人工审核,对高风险内容进行多重把关,并且在各个目标市场建立由本地专家组成的审核团队,确保对文化细微差异的准确理解。同时,应当建立便捷的用户反馈通道,及时收集和响应不同国别用户对内容的意见,开发可快速更新的动态规则机制,以适应不断变化的法规和社会期望。

(三)开发跨文化沟通和培训方案

在人工智能产品全球化的浪潮中,开发和实施有效的跨文化沟通和培训计划已成为企业提升国际竞争力的关键战略,其重要性不言而喻。通过系统性地培养员工的文化智商(CQ),企业可以显著增强其在多元文化环境中的适应能力和创新潜力,从而更好地把握全球市场机遇,正如IBM、宝洁和可口可乐等跨国巨头的成功实践所证明的那样。IBM推出的综合培训计划不仅提高了员工满意度,还加强了全球团队协作;宝洁针对不同市场设计的培训课程则帮助员工更好地应对文化差异,与各地合作伙伴建立了稳固关系;而可口可乐的跨文化培训计划则为其本土化品牌策略和客户关系提升提供了有力支撑。这些案例均充分说明了跨文化培训对企业全球运营的积极影响。

文化智商(CQ)作为个人在文化多样性环境中有效适应和应对的能力,其重要性已得到学界和业界的广泛认可。David Livermore 博士强调的文化智商四个关键维度——动机、知识、策略和行动,为企业提供了提升跨文化适应能力的具体方向,而 Patty Goodman 教授则进

一步指出了理解文化差异对于建立信任、促进合作的重要性。在技术支持方面,人工智能翻译工具如DeepL Translator和Microsoft Translator,以及SC Training等AI驱动的培训平台,为跨文化沟通和培训提供了强有力的技术支撑,使得企业能够更加精准、高效地开展跨文化培训,克服语言障碍,提高培训效果。联合利华运用AI技术分析本地消费者情感并调整营销策略的做法,更是展示了技术在跨文化商业实践中的创新应用。综上所述,通过系统性的跨文化培训计划,结合文化智商的培养和先进技术的应用,企业将能够更好地培养具备跨文化适应力的团队,制定有效的国际化战略,从而在全球人工智能市场中赢得更大的成功。

三、人工智能产品未成年人保护合规要点

(一)各国未成年人保护合规要求概述

在人工智能产品的未成年人保护方面,各国和地区都制定了相应的法规和指南,尽管具体要求有所不同,但都体现了对未成年人权益的特别关注。美国的《儿童在线隐私保护法案》(COPPA)针对13岁以下儿童,要求网站运营商在收集儿童个人信息时必须遵循公开原则和“父母可证实的同意”原则。该法案还规定了安全港计划,允许行业自律与立法相结合。

欧盟《通用数据保护条例》(GDPR)为全球树立了新标准,明确规定儿童个人数据值得特别保护。基于GDPR,英国制定了《适龄设计守则》(Age Appropriate Design Code, AADC),适用于可能被儿童(0-17岁)访问的所有在线服务。AADC提出了15个标准,包括儿童最大利益优先、默认高隐私设置、数据最小化等原则,强调产品设计应考虑不同年龄段儿童的需求。瑞典发布的《数字平台中儿童与青少年的权利:利益相关者指南》(The Rights of Children and Young People on Digital Platforms: A Stakeholder Guide)虽然不像其他国家的标准那么严格,但也强调了保护儿童免受有害媒体曝光的重要性。荷兰的《儿童权利准则》(Code for Children's Rights)提出了10项基本原则,包括允许儿童参与设计过程、避免对儿童进行数据分析和经济剥削等。爱尔兰数据保护委员会制定的《面向儿童的数据处理方法的基本要求》(Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing)提出了14项基本要求,强调了基础性保护、明确同意、零干扰等原则,并特别指出获得同意不应成为将儿童视为成年人的理由。

上述法规和指南共同体现了以下几个关键趋势:首先,未成年人年龄界定趋向宽泛,多数国家将18岁以下人群纳入保护范围;其次,强调数据收集和处理的最小化原则、透明度原则和父母同意原则;再次,特别关注地理位置信息、用户画像和行为广告等敏感领域;最后,要求进行数据保护影响评估,并实施诸如内容过滤、家长控制等特殊保护措施。

(二)人工智能产品对未成年人的潜在影响

人工智能产品对未成年人的认知发展和学习能力可能产生显著影响。智能玩具如编程机器人和智能积木有助于培养逻辑思维和问题解决能力,而智能学习平板和人工智能辅导应用通过个性化内容可以提高学习效率和兴趣。然而,这些产品也可能带来潜在风险。过度依

赖人工智能设备可能抑制独立思考和创造力,特别是当人工智能总是提供即时答案时。此外,人工智能驱动的个性化推荐系统可能导致信息茧房,限制未成年人接触多元信息的机会,从而影响其全面发展。

在社交能力和心理健康方面,人工智能产品的影响是双面的。智能教育机器人和对话机器人可以帮助未成年人练习语言表达和社交互动,智能健康手环则可以监测和改善身心健康。然而,长期与人工智能互动可能导致未成年人难以适应真实人际交往的复杂性,影响社交技能的全面发展。过度依赖人工智能设备还可能导致注意力分散、沉迷行为,甚至影响自我认知和情感发展。更深层次的影响还包括人工智能系统决策和推荐中可能包含的潜在偏见或固有观念,这些可能会被未成年人不加批判地接受,影响其价值观和世界观的形成。

隐私安全和教育公平是人工智能产品对未成年人影响的另两个重要方面。智能设备和穿戴设备收集了大量个人数据,包括位置信息、健康数据和行为模式,这些数据如果被不当使用或泄露,可能对未成年人的安全和隐私构成威胁。在教育公平方面,尽管人工智能产品可以提供个性化学习体验,但也可能加剧数字鸿沟。那些无法获得先进人工智能教育工具的未成年人可能在学习机会上处于劣势,这种不平等可能会随着人工智能技术在教育领域的深入应用而进一步扩大。因此,在开发和使用针对未成年人的人工智能产品时,需要全面考虑这些潜在影响,采取适当的保护措施,以确保技术进步能够公平地造福于所有未成年人。

(三)企业未成年人保护机制的设计与实施

在设计和实施未成年人保护机制时,企业需要考虑多个方面,并根据不同国家和地区的法规要求进行调整。首先,数据收集和处理原则是核心要素。如果企业计划在美国部署人工智能产品,需要遵循《儿童在线隐私保护法案》(Children's Online Privacy Protection Act, COPPA)的规定,对13岁以下儿童的个人信息采取特殊保护措施。这包括实施"父母可证实的同意"原则,在收集儿童个人信息前获得父母明确同意,并提供明确的隐私政策链接。同时,企业应采取数据最小化原则,只收集必要的信息,并确保数据的安全存储和使用。

其次,产品设计应考虑年龄适当性和隐私保护。如果企业计划在英国提供服务,需要遵循《适龄设计守则》(Age Appropriate Design Code, AADC)的要求。这意味着企业需要为不同年龄段的未成年人提供适当的内容和功能,并默认采用高隐私设置。例如,地理位置功能应默认关闭,用户分析和个性化推荐等功能应受到限制。此外,企业应提供清晰、易懂的隐私信息,使用儿童友好的语言和设计,帮助未成年人理解数据使用方式。

最后,企业需要建立全面的风险评估和管理机制。如果企业计划在欧盟国家运营,需要遵循GDPR的规定,进行数据保护影响评估(Data Protection Impact Assessment, DPIA)。这一过程应特别关注人工智能技术对未成年人权益的潜在影响,包括但不限于隐私风险、内容适当性、行为广告影响等。企业还应建立有效的内部控制机制,定期审查和更新保护措施,并为员工提供相关培训。同时,应考虑引入家长控制功能,让父母或监护人能够监督和管理未成年人的在线活动。此外,企业应建立便捷的用户反馈和投诉机制,及时响应未成年人及其监护人的顾虑,并在必要时提供数据访问、更正和删除的选项。通过这些综合措施,企业可以构建一个更安全、更负责任的人工智能产品环境,更好地保护未成年人的权益。

第四篇 人工智能产品出海之特殊行业合规要点

一、医疗行业中人工智能产品的合规要点

(一)医疗人工智能产品的监管框架与认证要求

1.监管框架及要求

在人工智能企业出海的背景下,医疗人工智能产品的监管框架与认证要求呈现出全球性的复杂格局,其中各国监管机构针对这一新兴技术领域制定了一系列严格而又灵活的规范,以确保产品的安全性、有效性和质量。在这一监管体系中,美国食品药品监督管理局(U.S. Food and Drug Administration, FDA)、欧洲药品管理局(European Medicines Agency, EMA)、日本医药品医疗器械综合机构(Pharmaceuticals and Medical Devices Agency, PMDA)以及加拿大卫生部(Health Canada)等机构扮演着关键角色,其各自制定的政策和指南不仅塑造了本国市场,还对全球医疗人工智能产品的发展轨迹产生了深远影响。

美国食品药品监督管理局(U.S. Food and Drug Administration, FDA)作为全球医疗监管的领头羊,其对医疗人工智能产品的监管思路尤为值得关注。该机构采用了基于风险的分层监管方法,并通过一系列指导文件不断完善其监管框架。美国食品药品监督管理局(U.S. Food and Drug Administration, FDA)发布的《人工智能和机器学习作为医疗设备软件行动计划》(Artificial Intelligence/Machine Learning (AI/ML) –Based Software as a Medical Device Action Plan)文件为业界提供了清晰的定义和实例,阐明了AI/ML技术如何在医疗设备中应用以及由此可能带来的变革。该计划涵盖了良好机器学习实践、预定变更控制计划以及透明度等关键议题,表明FDA正寻求构建一个既能确保产品安全有效,又能适应AI/ML技术快速迭代特性的监管生态系统。FDA于2024年3月发布的《人工智能与医疗产品:CBER、CDER、CDRH和OCP如何协同工作》(Artificial Intelligence and Medical Products: How CBER, CDER, CDRH, and OCP are Working Together)文件,说明FDA正在推动跨部门协作,以实现对医疗人工智能产品更全面、协调的监管。

在欧洲,欧洲药品管理局(European Medicines Agency, EMA)及其指定的认证机构负责监管医疗人工智能产品,其监管框架以欧盟《医疗器械法规》(Medical Device Regulation (MDR) (EU) 2017/745)为基础,要求产品根据风险等级进行分类并获得CE标志,体现了欧盟在确保产品安全性的同时,也注重维护单一市场的统一性。日本医药品医疗器械综合机构(Pharmaceuticals and Medical Devices Agency, PMDA)则通过发布针对《软件作为医疗设备的指南》(Guidance On Software as a Medical Device, SaMD),为该国医疗人工智能产品的开发和应用提供了明确的监管方向。

2.合规要点

针对我国人工智能相关企业在医疗领域的出海战略,结合前述监管框架与认证要求,可提炼出以下关键合规要点,以期为企业在国际市场的合规实践提供切实可行的指导:首先,企业应当深入理解并严格遵循目标市场的分层监管策略,尤其是美国FDA所倡导的基于风险的监管方法,在产品开发初期即应进行全面的风险评估,并据此制定相应的合规策略,确保产品设计与监管要求的高度契合;其次,鉴于AI/ML技术的迭代特性,企业需建立健全的变更管理机制,包括但不限于制定预定变更控制计划,以适应FDA等监管机构对AI/ML驱动软件的监管方法,同时,上述机制的建立也有助于企业在技术快速发展的背景下保持合规的灵活性和前瞻性;再者,企业应当高度重视产品的透明度问题,不仅要在技术层面确保人工智能算法的可解释性,还应在操作层面建立完善的文档管理系统,详细记录产品开发、测试和性能评估的全过程,以满足监管机构对医疗人工智能产品透明度的要求;最后,考虑到不同国家和地区在医疗人工智能产品监管方面的差异,企业应建立专门的跨区域合规团队,密切关注各目标市场的监管动态,如欧洲药品管理局(European Medicines Agency, EMA)对CE标志的要求、日本医药品医疗器械综合机构(Pharmaceuticals and Medical Devices Agency, PMDA)针对软件作为医疗设备的特殊指南等,并据此及时调整合规策略。

(二)医疗数据隐私保护与安全合规

医疗数据隐私保护与安全合规在人工智能产品出海过程中扮演着关键角色,其重要性不仅体现在满足法律法规要求上,更关乎患者权益和企业声誉。以美国《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996, HIPAA)为例,该法案为受保护健康信息(Protected Health Information, PHI)的收集、使用、处理和存储等环节制定了严格的国家标准,要求涵盖实体(Covered Entities, CE)和商业伙伴(Business Associates, BA)在处理可识别个人的健康信息时,必须采取周密的物理、管理和技术保障措施,确保信息的完整性和安全性。因此,在将人工智能技术应用于医疗领域时,企业需要特别注意《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996, HIPAA)隐私规则和安全规则的要求。

利用医疗数据训练人工智能模型的另一个关键环节是数据的去识别化处理。《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996, HIPAA)法案明确规定,经过去识别化处理的健康信息不再被视为PHI,可以更自由地被使用。然而,值得注意的是,即使在应用人工智能技术时,也不能默认患者的医疗健康信息可以被用于模型训练或优化。企业在使用患者数据前,必须获取明确的知情同意。这不仅是法律要求,也是体现尊重患者隐私权的考量。同时,在进行数据去识别化时,企业需要采用《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996, HIPAA)规定的专家确认或安全港方法,确保在保留数据价值的同时,将个人识别风险降至最低。

《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996, HIPAA)安全规则要求企业对电子形式的受保护健康信息采取严格的保护措施,企业需要通过高强度的加密技术保护存储的患者健康数据,同时构建严密的网络安全防护体系,并对人工智能模型本身进行安全工程,以降低黑客攻击和数据泄露的风险。特别是在云环境中

部署人工智能系统时,企业需要确保云服务提供商能够满足《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)的要求,并签订相应的商业伙伴协议(Business Associate Agreement,BAA)。出海的医疗相关人工智能企业在选择目的地国家时,要关注如美国《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)等具有本地特殊化的医疗数据合规要求,在做好战略预判的同时,准备相应的战术应对措施。

(三)人工智能辅助诊断与治疗的合规

人工智能在医疗辅助诊断与治疗方面的应用,正在逐步走向现实。其中的相关挑战不仅涉及技术层面,更触及了伦理、法律和社会等多个维度。在当前的医疗实践中,人工智能生成的医疗建议已经开始发挥重要作用,但其使用必须谨慎而有度。医疗机构在整合人工智能系统时,需要特别注意避免将人工智能生成的建议在缺乏适当背景的情况下直接呈现给患者。相反,该类建议应被视为增强医疗专业人员判断力的工具,而非取而代之的替代品,既需要体现对患者知情权的尊重,也应凸显人类医生在诊疗过程中不可或缺的核心地位。

为应对上述挑战,业界正在积极探索和构建新的伦理框架,例如,“GREAT PLEA”(Governability, Reliability, Equity, Accountability, Traceability, Privacy, Lawfulness, Empathy, and Autonomy)原则为医疗人工智能应用提供了伦理指导,涵盖了从可治理性到自主性等多个关键因素,其不仅强调了人工智能系统运作的透明度和问责制,还特别强调了尊重患者自主权的重要性。

在数据偏见风险管理方面,使用存在偏见的数据集训练人工智能系统可能导致诊断和治疗建议中出现系统性的不准确,其不准确性往往对特定群体造成不成比例的影响。为了缓解相关风险,医疗相关的人工智能企业需要采取多管齐下的策略。首先,应当构建多元化的训练数据集,确保数据能够充分代表不同人群的特征。其次,建立长期的偏见/歧视检测机制,定期评估人工智能系统的输出结果是否存在歧视性倾向。最后,加强对医疗从业者的培训,提高从业者识别和应对人工智能系统潜在偏见的能力。上述措施的实施不仅有助于提升人



工智能辅助诊断与治疗的准确性和公平性,也是确保医疗人工智能系统符合《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)等相关法规要求的关键所在。

2.合规要点

针对我国人工智能相关企业在医疗数据隐私保护与安全合规领域的国际化进程,结合前述《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)等法规要求,可梳理出以下核心合规要点,旨在为企业在全球医疗数据处理实践中提供切实可行的指导:第一,企业应当建立全面而严格的数据治理体系,该体系不仅要涵盖数据收集、使用、存储和传输等全生命周期管理,还需特别关注跨境数据流动的合规问题,确保企业的数据处理活动始终符合《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)等国际通行标准;第二,鉴于医疗数据的高度敏感性,企业必须实施强有力的技术保护措施,包括但不限于采用高强度加密技术保护存储和传输中的患者健康数据,构建多层次的网络安全防护体系,并对人工智能模型本身进行全方位的安全工程,以最大程度降低数据泄露和黑客攻击的风险;第三,企业应当建立健全的内部合规培训机制,确保所有接触医疗数据的员工充分了解相关法律法规的要求,尤其是《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)对受保护健康信息(Protected Health Information,PHI)处理的严格规定,并能在日常工作中严格执行相关合规程序;第四,考虑到数据去识别化在人工智能模型训练中的关键作用,企业需要制定详细的数据去识别化流程和标准,严格遵循HIPAA规定的专家确认或安全港的处理方法,在保留数据价值的同时最大限度地降低个人识别风险;第五,企业还应建立完善的知情同意机制,在使用患者数据进行模型训练或优化之前,必须获取明确的知情同意,这不仅是法律要求,更是尊重患者隐私权的重要体现;第六,针对云环境下的人工智能系统部署,企业需要特别注意选择符合《健康保险携带和责任法案》(Health Insurance Portability and Accountability Act of 1996,HIPAA)要求的云服务提供商,并与之签订严格的商业伙伴协议(Business Associate Agreement,BAA),明确双方在数据保护方面的责任和义务,同时定期对云服务提供商的合规状况进行审核,以确保整个数据处理链条的安全性和合规性。从而为我国人工智能企业在全全球医疗数据市场建立起坚实的合规防线,为企业的长远发展和国际化战略保驾护航。

二、金融行业中人工智能产品的合规要点

在全球金融科技浪潮的推动下,更多人工智能企业正积极寻求国际市场的发展机遇。随着彭博社 BloombergGPT、微软 Azure OpenAI 等金融专用大模型的崛起,以及英国 Atom、德国 Neos 等虚拟银行的成功实践,国际金融市场对人工智能技术的需求日益旺盛。麦肯锡的调查显示,超过半数的欧美大型金融机构已采用集中化结构来部署通用人工智能技术,涵盖数据分析、风险管理等多个领域。面对这一趋势,人工智能企业在出海过程中不仅要把握技术创新和效率提升的机遇,更要严格遵守目标市场的金融监管法规。本节将聚焦金融人工智

能产品的合规要点,涉及应用规范、数据使用和决策透明度等关键问题,为人工智能企业在国际金融市场的合规实践提供重要参考。

(一)人工智能在金融服务中的应用合规

人工智能在金融服务中的应用合规已成为全球金融监管机构的重点关注领域,其中美国证券交易委员会(U.S. Securities and Exchange Commission, SEC)和英国金融行为监管局(Financial Conduct Authority, FCA)的监管举措尤为值得关注。SEC近期在监管人工智能在投资咨询服务中的使用方面采取了积极行动,对两家投资顾问公司的“AI 洗白”行为展开执法,这标志着美国证券交易委员会(U.S. Securities and Exchange Commission, SEC)对人工智能在金融领域应用的监管进入了新阶段。SEC的执法行动不仅涉及具体的民事罚款,还启动了专门的“AI 专项调查”,并进一步制定新的规则以规范预测性数据分析的使用。与此同时,英国金融行为监管局(Financial Conduct Authority, FCA)制定的金融服务人工智能使用原则为全球金融机构提供了重要参考。英国金融行为监管局(Financial Conduct Authority, FCA)特别强调了透明性、公平性和责任制三大核心原则,要求金融机构确保人工智能使用的透明度,防止人工智能系统产生歧视或偏见,并对人工智能决策承担责任。

对于计划进军国际市场的人工智能企业而言,企业需要避免在营销材料中对人工智能能力作出误导性陈述,确保人工智能系统的实际功能与宣传一致。同时,企业还应建立健全的内部控制机制,确保人工智能系统的公平性、透明度和可解释性,并准备好应对可能的监管审查。此外,人工智能企业还需要关注SEC正在制定的新规则,特别是关于管理预测性数据分析相关利益冲突的要求。企业应提前布局,建立相应的合规体系和书面政策,以满足未来可能出台的监管要求。

(二)金融相关数据的合规使用

金融相关数据的合规使用是人工智能在金融服务领域应用的核心挑战之一,涉及复杂的法律法规和严格的监管要求。在这一领域,《通用数据保护条例》(General Data Protection Regulation, GDPR)和《加利福尼亚消费者隐私法》(California Consumer Privacy Act, CCPA)等法规为数据处理设定了高合规标准,要求金融机构在使用人工智能技术时必须严格保护客户隐私和数据安全。然而,合规挑战远不止于此。金融机构还需要遵守《多德-弗兰克法案》(Dodd-Frank Act)和反洗钱(Anti-Money Laundering, AML)法规等一系列具体规定,上述法规对人工智能系统在风险评估、决策和可疑活动检测方面提出了明确要求。在实践中,金融机构面临的主要合规问题包括数据隐私保护、数据安全维护、数据的科技伦理使用以及保持人工智能操作的透明度和责任制,要求机构在收集和处理数据时遵循数据最小化原则,获取客户明确同意,并建立有效的数据泄露报告机制。近年来,引起广泛关注的几起合规失败案例,如Capital One的数据泄露事件和法国农业信贷银行在反洗钱(Anti-Money Laundering, AML)实践方面的不足(导致其面临严重的合规风险和监管处罚),凸显了合规风险的严重性和监管执法的力度。

结合前述GDPR、CCPA等法规要求,可总结出以下关键合规要点:首先,企业应当建立全

面的数据分类和标记机制,严格遵循数据最小化原则;其次,构建健全的客户同意管理系统,确保在收集和使用个人金融数据时获取明确同意;再者,制定严格的跨境数据传输政策,评估目标国家的数据保护水平,采取适当措施确保数据传输的合法性和安全性;此外,建立完善的数据泄露应对机制,包括制定详细的检测、报告和处理流程;最后,设立专门的合规监测团队,持续关注全球金融数据保护法规的最新发展,及时调整内部政策和实践,以适应不断变化的监管环境,为企业在国际金融市场的稳健发展奠定合规基础。

(三)人工智能辅助金融决策的透明度要求

人工智能辅助金融决策已成为全球金融监管的焦点,反映了监管机构对人工智能系统公平性和可解释性的高度重视。美国消费者金融保护局(U.S. Consumer Financial Protection Bureau, CFPB)明确强调,现有法律如《平等信贷机会法》(Equal Credit Opportunity Act, ECOA)完全适用于金融领域的人工智能应用,要求金融机构对不利决策提供明确解释,并确保遵守公平贷款法律。2023年美国政府发布《关于安全、可靠和可信赖人工智能的行政命令》(Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence)进一步强化了上述要求,指示监管机构评估人工智能工具在贷款和信贷决策中的潜在偏见。

为满足透明度要求,金融机构需要实施一系列措施。首先,机构必须定期对人工智能模型进行偏见测试,检查是否存在基于种族、性别或社会经济地位的歧视性决策。其次,机构需要保持详细的文档记录,明确说明人工智能系统中个人数据的使用情况,包括数据来源、处理方式和使用目的。此外,向客户提供易于理解的解释,阐明人工智能系统如何影响决策过程,也是透明度要求的重要组成部分。

法律义务方面,当金融机构拒绝信贷或采取不利行动时,必须根据《平等信贷机会法》(Equal Credit Opportunity Act, ECOA)等法律提供具体理由,上述要求同样适用于人工智能



驱动的决策过程。美国消费者金融保护局(U.S. Consumer Financial Protection Bureau, CFPB)特别强调,算法决策可能导致歧视性结果,如管理不当可能违反民权法,因此机构需要持续监控人工智能系统,防止潜在的不公平待遇。近年来,一些案例研究显示某些信用评分模型可能对特定群体存在歧视性结果,同时,针对违反公平贷款法律的自动化决策流程,美国的相关监管机构也已采取具体执法行动。

基于前文所述的监管要求和行业实践,我国人工智能相关企业在应对金融决策透明度挑战时,应着重关注以下合规要点:

其一,开发可解释的人工智能模型,确保决策过程的可追溯性和可审核性。其二,建立定期的偏见测试机制,防范基于种族、性别等因素的歧视性决策。其三,完善数据使用文档体系,详细记录个人数据的来源、处理方式和使用目的。其四,设计用户友好的解释界面,向客户清晰阐明人工智能系统如何影响决策结果。其五,制定符合 ECOA 等法规的不利行动通知流程,为被拒绝的申请提供具体理由。

三、制造业中人工智能产品的合规要点

(一)制造业中人工智能产品的合规框架与要求

制造业中人工智能产品的合规要点涉及多个层面,包括安全标准、数据保护以及特定行业的规范。以下将从智能制造系统的安全标准与认证要求、工业数据收集、隐私保护合规,以及工业机器人和自动化设备的合规三个方面进行阐述,并以带有人工智能车机系统的制造业出海为例进行说明。

在智能制造系统的安全标准与认证要求方面,美国和欧盟都制定了严格的规范。美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)发布的《人工智能风险管理框架》(Artificial Intelligence Risk Management Framework)为制造业人工智能系统的安全性提供了重要指导。该框架强调了人工智能系统在设计、开发和部署过程中的风险评估和管理。欧盟方面,《机械指令》(Machinery Directive 2006/42/EC)及其即将实施的更新版本对包含人工智能组件的制造设备提出了具体要求,涵盖了从风险评估到安全控制系统的各个方面。

对于工业数据收集与隐私保护合规,欧盟的《通用数据保护条例》(General Data Protection Regulation, GDPR)对制造业企业在数据处理方面提出了严格要求。即使在工业环境中,涉及个人数据的收集和处理也必须遵守 GDPR 的规定,包括数据最小化原则和获得明确同意等。美国虽然没有统一的联邦级数据保护法,但加利福尼亚州的《消费者隐私保护法案》(California Consumer Privacy Act, CCPA)等州级法律对制造企业的数实践也有重要影响。

工业机器人和自动化设备的合规主要涉及安全性和互操作性。国际标准化组织(ISO)的 ISO 10218 标准系列为工业机器人的安全要求提供了全面指南。此外,美国职业安全与健康管理局(Occupational Safety and Health Administration, OSHA)的相关规定也对工业自动

化设备的安全操作提出了具体要求。在欧盟,除了前述的《机械指令》(Machinery Directive, 2006/42/EC)外,《无线电设备指令》(Radio Equipment Directive, RED)对具有无线通信功能的工业设备也有特定规定。

以带有人工智能车机系统的制造业出海为例,企业面临的合规挑战尤为复杂。首先,车载人工智能系统必须符合目标市场的汽车电子标准,如美国的FMVSS《联邦机动车安全标准》(Federal Motor Vehicle Safety Standards, FMVSS)和欧盟的ECE (Economic Commission for Europe)法规。其次,系统涉及的数据收集和处理必须遵守GDPR等隐私保护法规,特别是在处理位置数据和驾驶行为数据时。再者,人工智能系统的决策过程必须具有可解释性和透明度,以满足潜在的监管审查。

此外,车载人工智能系统的网络安全也是重要考量。美国国家公路交通安全管理局(National Highway Traffic Safety Administration, NHTSA)发布的网络安全最佳实践指南和联合国欧洲经济委员会(United Nations Economic Commission for Europe, UNECE)的WP.29法规对车辆网络安全提出了具体要求。制造商需要确保人工智能系统能够抵御潜在的网络攻击,并且能够及时更新以应对新出现的威胁。在生产过程中,制造商还需要考虑人工智能系统的可追溯性和质量控制,其涉及传统的质量管理体系(如ISO 9001)还包括针对人工智能系统的特定质量保证措施。例如,确保人工智能模型的训练数据质量、模型性能的稳定性,以及在不同环境条件下的可靠性。

(二)合规要点

针对我国人工智能相关企业在制造业领域的国际化进程,结合前述安全标准、数据保护及特定行业规范,可提炼出以下关键合规要点:首先,企业应当建立全面的风险评估和管理体系,参考NIST的《人工智能风险管理框架》,确保人工智能系统在设计、开发和部署各阶段的安全性;其次,针对欧盟市场,企业需特别关注《机械指令》的要求,对包含人工智能组件的制造设备进行全面的安全评估和控制;再者,建立严格的数据治理机制,即使在工业环境中,也要确保个人数据的收集和处理符合GDPR等隐私保护法规的规定;此外,企业应当重视工业机器人和自动化设备的安全性和互操作性,严格遵守ISO 10218标准系列和OSHA的相关规定。

就带有人工智能车机系统的制造业而言,企业还需注意以下要点:首先,确保车载人工智能系统符合目标市场的汽车电子标准,如美国的FMVSS和欧盟的ECE法规;其次,建立完善的数据保护机制,特别是在处理位置数据和驾驶行为数据时,严格遵守GDPR等隐私法规;再者,提高人工智能决策过程的可解释性和透明度,以应对潜在的监管审查;此外,强化车载人工智能系统的网络安全防护,遵循NHTSA的网络安全最佳实践指南和UNECE的WP.29法规;最后,建立人工智能系统的质量控制和可追溯机制,结合传统的ISO 9001质量管理体系,确保人工智能模型训练数据质量和性能的稳定性。



数据 合规

第五章

第一篇 企业境外经营过程中的数据合规要点

随着人工智能技术的快速发展,大模型企业纷纷将目光投向海外市场,寻求新的增长机遇。然而,在这片充满潜力的蓝海中,数据合规问题成为企业出海过程中不可忽视的关键挑战。本文旨在探讨大模型企业在海外市场开展业务过程中所面临的数据合规问题,首先企业应准确识别在目标市场所适用的数据法规,其次企业应根据适用法规的要求构建公司内部数据合规体系,最后企业应尤其重视在具体运营中对用户信息的保护。

一、目标市场适用数据法规的识别

为了在目标市场合法、有效地开展业务,企业首先需要准确识别适用的数据法规。这个过程不仅关乎企业的合规风险管理,更是制定有效业务策略的基础。以下从企业在目标市场是否设立主体这两种不同情形进行分析。

(一)在目标市场设立主体

在目标市场设立主体的情况下,企业极大可能受到该目标市场数据隐私法律的规制。以欧盟的《通用数据保护条例》(General Data Protection Regulation, GDPR)为例,首先,数据控制者和数据处理者在欧盟境内设立机构,其活动范围内所进行的数据处理行为,不论该处理行为是否发生在欧盟境内,都将受到GDPR的规制。其次,虽然设立于欧盟境外,但根据国际公法的规定适用欧盟成员国法律的数据控制者所进行的个人数据处理行为,同样需要遵守GDPR。这意味着,一旦企业在欧盟设立了主体并进行数据处理,无论数据实际上在哪里被处理,都将不可避免地受到GDPR的约束。

(二)在目标市场未设立主体

然而,即使企业在目标市场未设立主体,也并不意味着可以完全规避当地的数据保护法规。在这种情况下,企业需要特别注意其用户所在地和数据处理所在地的法律规定。再以GDPR为例,其明确指出,当设立于欧盟境外的数据控制者和处理者对位于欧盟境内的数据主体的个人数据进行处理时,如果是为了向这些欧盟境内的数据主体提供货物或服务(无论是否要求付费),或者对这些数据主体在欧盟境内的行为进行监控,都将受到GDPR的管辖。这种域外适用的规定大大扩展了GDPR的适用范围,使得许多未在欧盟设立实体的企业也需要遵守其规定。

同时,企业还需要考虑数据跨境流动可能带来的额外合规要求,如果企业将境外收集的数据传输到中国境内进行处理,根据中国《个人信息保护法》的规定,只要是在中华人民共和国

国境内处理自然人个人信息的活动,就必须遵守该法的规制。这意味着,即使数据来源于境外,一旦进入中国进行处理,就会触发中国数据保护法的适用。

需要注意的是,企业除了从主体角度进行识别,还需要结合具体的行业领域、业务场景和数据处理场景进行全面分析,金融、医疗、教育等敏感行业通常面临更严格的数据保护规定。例如,美国的《健康保险可携性和责任法案》(Health Insurance Portability and Accountability Act, HIPAA)专门规范医疗健康数据的处理,而《格拉姆-里奇-比利雷法案》(Gramm-Leach-Bliley Act, GLBA)则针对金融机构的客户信息保护。大模型企业若涉足这些行业,除需遵守一般数据保护法规外,还必须符合行业特定的合规要求。

针对法律适用情况的判断,首先,企业需要对其全球业务进行详细的数据映射,清晰地了解数据的收集、处理、存储和传输路径。其次,企业应该针对每个目标市场进行深入的法律分析,不仅要考虑自身是否在当地设立了实体,还要评估其数据处理活动是否针对了当地用户,或是否监控了当地用户的行为。此外,企业还需要关注数据跨境流动以及特定行业可能触发的额外法律要求。

二、公司内部数据合规体系的构建

在确定适用的数据法规后,企业需要根据法规的要求构建健全的内部数据合规体系。建立合规体系不仅是满足法律要求的必要措施,更是企业在国际市场中赢得信任、实现可持续发展的关键。企业可从以下两个核心方面开展:设置数据安全管理机构与负责人,以及建立完善的数据安全保护制度。

(一)设置数据安全管理机构与负责人

设置数据安全管理机构与负责人是构建内部数据合规体系的首要任务。此过程需要企业根据自身规模、业务性质以及目标市场的法律要求,建立一个专门的组织架构。对于大型跨国企业而言,可成立一个独立的数据合规部门,由高级管理层直接领导,能够跨部门协调,推动全公司范围内的数据合规工作。

在此架构中,任命一位首席数据合规官(Chief Data Compliance Officer, CDCO)或数据保护官(Data Protection Officer, DPO)至关重要。此角色需要由具备深厚法律和技术背景的专业人士担任,不仅要熟悉各个目标市场的数据保护法规,还要了解企业的技术架构和数据处理流程。CDCO 或 DPO 的主要职责包括制定公司的数据合规策略,监督合规措施的实施,处理数据主体的请求和投诉,以及与监管机构保持沟通,作为数据合规工作主要责任人、牵头人,对企业负责人负责,专管企业数据合规全流程。

值得注意的是,一些法域(如欧盟的 GDPR)明确要求特定类型的企业必须任命 DPO。即使在没有强制要求的市场,设立这样一个角色也能显著提升企业的合规能力和公信力。此外,企业还需要在各个业务部门指定数据保护联络人,作为部门与数据合规团队之间的桥梁,确保合规要求能够有效落实到日常运营中。

(二)建立数据安全保护制度

建立健全的数据安全保护制度是内部合规体系的另一个关键支柱。数据安全保护制度应涵盖数据生命周期的各个阶段,以在数据收集、数据传输、数据存储、数据使用、数据交换、数据删除等各阶段有效保护数据安全为基础开展相应工作。

企业需要制定清晰的数据收集规则,明确规定哪些数据可以收集,如何获取用户同意,以及数据可以用于哪些目的。

数据传输环节是数据安全的重要关口。企业需要建立严格的数据传输协议,确保数据在网络传输过程中的安全性,例如使用加密技术、安全传输协议(如HTTPS),以及实施访问控制机制。对于跨境数据传输,还需要特别考虑目标国家的数据本地化要求和跨境传输限制,制定相应的合规策略。

企业需要建立严格的数据存储、访问控制机制。这包括实施最小权限原则,确保数据存储于安全环境、严格控制访问权限,即员工只能访问履行职责所必需的数据,以及建立多因素认证、定期权限审核等技术措施。同时,企业还应该制定详细的数据分类标准,根据数据的敏感程度和重要性采取相应的保护措施。

在数据处理阶段,企业需要建立严格的数据访问控制机制,确保只有经授权的人员能够访问和处理相关数据。对于涉及自动化决策或用户画像的数据处理,还需要特别注意遵守相关法规(如GDPR)的要求。此外,企业应建立数据处理日志记录系统,以便追踪和审计数据的使用情况。

数据交换环节涉及与第三方的数据共享和交换。企业需要制定明确的数据共享政策,包括评估数据接收方的安全能力、签订数据保护协议,以及实施技术措施确保数据交换的安全性。对于涉及个人数据的交换,还需要确保获得数据主体的同意,并提供撤回同意的机制。

数据删除政策也是数据安全保护制度的重要组成部分。企业需要明确规定不同类型数据的保留期限,并建立自动化的数据删除机制,确保在法律要求的期限内妥善处理过期数据,以减少不必要的合规风险,优化存储资源的使用。

此外,企业还需要制定数据安全事件应对预案,详细规定发生数据安全事件时的报告流程、应对措施以及用户和监管机构的沟通方案。定期进行模拟演练可以帮助企业在实际发生数据安全事件时更快、更有效地做出反应。

员工培训和意识提升也是数据安全保护制度中不可或缺的一环。企业应该建立常态化的培训机制,确保所有员工都了解数据保护的重要性,熟悉公司的数据处理政策和程序。培训应该根据不同岗位的需求进行定制,并定期更新内容以反映最新的法律要求和技术发展。

为了确保数据安全保护制度的有效性,企业还需要建立定期的内部审计和评估机制,对数据处理活动进行全面梳理,评估现有措施的有效性,识别潜在的风险和改进空间。同时,聘请外部专家进行独立审计可以为企业提供更客观的评估和建议。

随着技术的快速发展和法规环境的不断变化,数据安全保护制度需要保持动态更新。企业应定期评估和修订相关政策和程序,以适应新的合规要求和安全挑战。

三、用户信息处理的原则与规范

企业必须严格遵循用户信息处理的原则与规范,重点关注三个方面:遵循处理用户个人信息的基本原则、规范用户个人信息的收集与处理,以及明确共享、转让用户个人信息的方式。

(一)遵循用户个人信息处理的原则

企业必须严格遵循所适用数据隐私法规中规定的个人信息处理原则。这些原则虽然在不同法域可能有细微差异,但核心内容基本一致。以GDPR为例,其中规定的原则包括合法性、公平性和透明度原则,目的限制原则,数据最小化原则,准确性原则,存储限制原则,完整性和保密性原则,以及问责制原则。这意味着企业在处理个人信息时,不仅要确保处理的合法性,还要保证整个过程对数据主体公平透明。企业必须明确界定数据处理的目的,并确保只收集和实现该目的所必需的数据。同时,企业还需要采取适当的技术和组织措施,保证数据的准确性、完整性和安全性。

企业应将个人信息处理的原则深深植入其数据处理的每个环节,从产品设计到日常运营。例如,企业在设计产品功能时,就应考虑个人信息的保护,如默认采用最高级别的隐私设置,或者为用户提供细粒度的数据控制选项。同时,企业还应该建立完善的内部审计机制,定期评估其数据处理活动是否符合这些原则,并及时纠正任何不合规的做法。

(二)规范用户个人信息的收集与处理

规范对用户个人信息的收集与处理是确保合规的关键环节。大模型企业通常需要处理大量个人数据以训练和优化模型,这使得规范数据收集和处理变得尤为重要。企业应该建立清晰的数据收集政策,明确界定哪些数据是必要的,哪些是可选的。在收集数据时,企业必须获得用户的明确同意,并提供清晰、易懂的说明,解释数据将如何被使用。

在数据处理方面,企业需要建立严格的数据访问控制机制,确保只有经过授权的人员才能访问用户的个人信息,且访问范围限定在履行职责所必需的程度。同时,企业应该实施数据最小化原则,只处理实现特定目的所必需的数据。例如,在训练语音识别模型时,可能只需要语音数据本身,而不需要保留用户的身份信息。此外,企业还应该采用高级的数据匿名化技术,在保护个人隐私的同时,最大化数据的使用价值。

对于用户的敏感个人信息,如生物特征数据、健康数据等,企业需要采取更加严格的保护措施。这可能包括使用高级加密技术,实施更严格的访问控制,或者在某些情况下完全避免处理此类数据。企业还应该定期进行数据处理影响评估(Data Processing Impact Assessment, DPIA),特别是在引入新技术或开展可能对个人权利构成高风险的数据处理活动时。

(三)明确共享、转让用户个人信息的方式

明确共享、转让用户个人信息的方式是保护用户权益、维护企业信誉的重要环节。在全

全球化的业务环境中,数据的跨境传输几乎是不可避免的。然而,不同国家和地区对数据出境有着不同的要求,企业必须谨慎处理。首要任务是通过隐私政策向数据主体清晰地说明数据可能被共享或转让的情况。隐私政策应该使用简单、明确的语言,确保大众能轻松理解。在隐私政策中,企业应该详细说明哪些类型的数据可能被共享或转让,共享或转让的目的是什么,可能的接收方是谁。如果涉及跨境数据传输,还需要说明数据可能被传输到哪些国家或地区,以及企业采取了哪些措施来保护数据。例如,如果企业使用标准合同条款(Standard Contractual Clauses, SCCs)或约束性公司规则(Binding Corporate Rules, BCRs)来确保跨境数据传输的合法性,应该在隐私政策中予以说明。

此外,企业还应该为用户提供控制其数据被共享或转让的选项。这可能包括允许用户选择退出某些类型的数据共享,或者要求在每次数据转让前获得用户的明确同意。对于那些必须进行的数据共享或转让(如为了履行合同义务或遵守法律要求),企业应该清楚地解释原因,并说明用户的权利可能受到哪些限制。

在实际操作中,企业需要建立严格的内部审批流程,确保每次数据共享或转让都经过充分的合规评估。流程应包括对接收方的尽职调查,确保他们能够提供足够的数据保护水平。同时,企业还应该与数据接收方签订详细的数据处理协议,明确规定双方的责任和义务,包括数据保护措施、数据使用限制、以及在发生数据泄露时的通知和协助义务。

(四)用户个人信息主体权利的保障

企业在海外业务运营中还应有效保障用户个人信息主体的权利,包括知情权、访问权和更正权、删除权,以及数据可携带权等。

1.知情权

知情权是用户个人信息保护的基础,也是其他权利行使的前提。企业应以清晰、易懂的方式向用户说明个人信息的收集、使用和处理情况。通常可通过产品隐私政策来实现,在用户注册或首次使用服务时,可以通过简洁的弹窗或交互式界面,突出显示关键的隐私信息。同时,企业还应该在数据收集的具体场景中提供即时的通知和解释,如在请求访问位置信息时说明用途和存储时间。

此外,当数据处理目的发生变化或企业引入新的数据使用方式时,应及时通知用户并在必要时重新获取同意。在这个过程中,企业需要特别注意不同文化背景和语言环境下的沟通效果,确保信息传达的准确性和有效性。

2.访问权和更正权

访问权和更正权赋予了用户查看和修改其个人信息的权利,这对于确保数据准确性和用户控制权至关重要。企业应该建立用户友好的机制,允许用户方便地查看企业所持有的关于他们的个人信息。在用户发现信息不准确或过时,企业应提供简单直接的更正途径。这不仅包括基本的个人信息,还应涵盖系统中的派生数据或推断数据。例如,如果系统基于用户行为数据做出了某些偏好推测,用户应该有权了解并更正这些推测。同时,企业需要建立内部机制,确保用户提出的更正请求能够及时、全面地在所有相关系统中得到反映。

3.删除权

删除权,也被称为“被遗忘权”,是数据保护法规中的一项重要权利。大模型企业在设计数据处理系统时,应该从一开始就考虑如何实现有效的数据删除,包括建立清晰的数据保留政策,明确不同类型数据的保留期限,并在期限到期后自动删除数据。当用户行使删除权时,企业应该能够快速响应,不仅删除直接存储的个人数据,还要考虑从派生数据和缓存中移除相关信息。

然而,用户删除权的保障在大模型企业中可能面临特殊挑战。例如,在深度学习模型中,个人数据可能已经被用于训练,简单删除原始数据可能无法完全消除其影响。在这种情况下,企业需要探索更先进的技术解决方案,以在保护个人隐私和维护模型性能之间取得平衡。同时,企业还需要清楚地向用户解释数据删除的范围和限制,确保用户理解他们的请求可能产生的影响。

4.数据可携带权

数据可携带权是近年来新兴的一项重要权利,旨在增强用户对其数据的控制,并促进市场竞争。大模型企业需要开发技术解决方案,允许用户以结构化、常用和机器可读的格式获取其个人数据,并将这些数据传输给其他服务提供商。这不仅包括用户直接提供的数据,还可能包括通过使用服务而生成的数据。

实现有效的数据可携带性需要企业在数据架构设计时就考虑其可操作性。例如,采用开放的数据标准和格式,确保数据能够在不同系统间易于交换和理解。同时,企业还需要建立安全的数据传输机制,如API接口,允许用户直接将数据传输到其他服务提供商。在实施过程中,企业应该平衡数据可携带性与数据安全性,确保在便利用户的同时不会增加数据泄露的风险。

同样地,对于大模型企业而言,数据可携带权的保障可能面临独特的挑战。例如,如何处理模型生成的洞察或预测结果,这些数据虽然与用户相关,但可能涉及企业的知识产权。在这种情况下,企业需要仔细权衡,找到既尊重用户权利又保护自身利益的平衡点。

为了有效实现这些权利保障,大模型企业需要建立一套完整的响应机制。这包括设立专门的团队处理用户请求,开发自动化工具加速请求处理过程,以及建立明确的时间表,确保在法定期限内回应用户请求。同时,企业还应该定期审查和更新这些机制,以适应不断变化的法律要求和用户期望。

从识别适用法规到构建内部合规体系,从遵循用户信息处理原则到保障用户权利,企业需要全方位应对复杂的数据治理环境。合规不应被视为束缚,而是企业提升竞争力的机遇。通过将数据保护融入产品设计和提供服务全过程,企业可以赢得用户信任,树立负责任的品牌形象。能在合规与创新间取得平衡的企业,将在数据驱动的全球经济中占据优势,为构建更安全、公平的数字世界做出贡献。

第二篇 大模型企业数据出境合规

随着大数据、人工智能等技术的飞速发展,大模型企业日益成为推动我国经济增长的重要力量。在全球化背景下,跨国企业间的数据交流与合作愈发频繁,数据出境问题逐渐成为大模型企业关注的焦点。本文旨在分析我国数据出境监管要求,探讨大模型企业在日常运营中可能涉及的数据出境场景以及我国数据出境的监管要求,并提出针对性的合规建议,助力大模型企业安全、合规地开展国际业务。

一、大模型企业主要数据出境场景

什么是“数据出境”?《数据出境安全评估申报指南(第二版)》第一条对数据出境行为进行定义:“以下情形属于数据出境行为:(一)数据处理者将在境内运营中收集和产生的数据传输至境外;(二)数据处理者收集和产生的数据存储在境内,境外的机构、组织或者个人可以查询、调取、下载、导出;(三)符合《个人信息保护法》第三条第二款情形,在境外处理境内自然人个人信息等其他数据处理活动。”需要注意的是,由中国内地向香港特别行政区、澳门特别行政区,以及台湾地区传输数据的行为亦属于数据出境,需接受监管。大模型企业在日常运营中主要涉及以下两种出境场景:

(一)使用境外算力

在生成式人工智能发展过程中,算力资源的重要性不言而喻。然而,由于国内相关基础设施建设的滞后以及国际贸易政策的限制,许多企业面临着算力不足的困境。为解决这一问题,一些企业选择跨境调用境外算力,但这种做法不可避免地会引发数据出境。

在此过程中,企业可能需要将在境内收集的大量语料(包括网络文章、社交媒体数据等)传输到境外的服务器上。模型训练在境外的服务器上进行,涉及的所有数据都暂时存储在境外。且训练完成后的模型参数和结构可能会被长期存储在境外的数据中心。

因此,在条件允许的情况下,企业可考虑优先使用国内算力资源或探索利用联邦学习等技术来减少数据出境的需求。

(二)调用境外模型

除了直接使用境外算力,许多企业选择通过调用成熟的境外模型来快速构建自己的应用。这种做法虽然能够大幅缩短研发周期,降低技术门槛,但同时也不可避免地引发了数据出境问题。

直接调用境外模型进行推理是最为典型和常见的情形,在此过程中,企业可能将用户的

查询、指令或其他输入数据实时传输至境外服务器,由部署在海外的模型进行处理和分析,随后将生成的结果返回给用户。此外,企业还可能利用境外模型进行微调 and 训练。例如,企业通过从境外采购云端私有化模型服务来支持自己反欺诈系统的运营。在前期,企业可能需要将大量的交易数据、用户行为数据以及历史欺诈案例数据传输到境外模型供应商的服务器上,这些数据将用于在基础模型上进行微调 and 训练,以适应中国特定的金融环境和欺诈特征。后期系统投入使用后,在每次进行欺诈检测时,实时的交易数据都需要发送到境外服务器进行分析,从而触发了持续的数据出境。

通过以上两个具体场景的分析,我们可以清楚地看到,在追求技术创新和效率的过程中,大模型企业很容易不经意间就触发数据出境。无论是为了获取更强大的算力资源,还是为了利用更先进的算法模型,数据的跨境流动似乎已成为一种难以避免的趋势。考虑到数据安全、隐私保护以及国家安全等多方面因素,企业在进行技术选型和业务决策时,必须充分考虑数据出境可能带来的潜在风险,并采取相应的保护措施。

二、我国对数据出境的法律监管

(一)我国数据出境所规制的数据类型

我国目前对数据跨境监管的数据类型主要分为重要数据和个人信息。因此,重要数据和个人信息的识别成为企业数据跨境合规工作的首要环节。

1.重要数据

将于2025年1月1日施行的《网络数据安全管理条例》,其第六十二条规定:重要数据,是指特定领域、特定群体、特定区域或者达到一定精度和规模,一旦遭到篡改、破坏、泄露或者非法获取、非法利用,可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。国家标准《数据安全技术 数据分类分级规则》(GB/T 43697-2024)为各行业和领域提供了数据分类分级的指导原则,并在附录G中详细阐述了重要数据的识别方法。

《规范和促进数据跨境流动的规定》(以下简称:《数据跨境新规》)第二条规定“数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的,数据处理者不需要作为重要数据申报数据出境安全评估。”此规定无疑为企业在数据跨境过程中减轻了部分合规负担,使得企业能够更为灵活地处理非明确界定为重要的数据。然而,这一规定并不等同于企业在面对数据跨境时可以完全忽视重要数据的监管要求。结合《信息安全技术 重要数据处理安全要求(征求意见稿)》及《工业和信息化领域数据安全管理办法(试行)》等文件的要求,企业在筹划数据跨境活动时,仍须识别自身业务中可能涉及的重要数据,并依据现行规定编制重要数据目录,适时向国家相关部门或本地区行业监管部门进行备案或上报的责任。

对于重要数据的识别,部分地区正在积极探索实施细则。天津自贸区发布的《中国(天津)自由贸易试验区企业数据分类分级标准规范》为企业数据的分类分级提供了具体指导;上海自贸区临港新片区则通过《中国(上海)自由贸易试验区临港新片区数据跨境流动分类分级

管理办法(试行)》,对数据跨境流动采取了更为细致的管理方法。北京自贸区在数据出境管理方面采取了更为创新的负面清单模式。《中国(北京)自由贸易试验区数据出境负面清单管理办法(试行)》和《中国(北京)自由贸易试验区数据出境管理清单(负面清单)(2024版)》的出台,标志着数据出境管理向更加明确和透明的方向迈进。地方性探索的深入和经验的积累,将为企业的出境活动提供更加清晰的指引。

2.个人信息

《中华人民共和国民法典》第一千零三十四条对个人信息进行定义:个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。《个人信息保护法》第四条规定,个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,匿名化处理后的信息不属于个人信息。

国家标准《信息安全技术 个人信息安全规范》中指出,判定某项信息是否属于个人信息,应考虑“识别”和“关联”两条路径:识别指从信息到个人,由信息本身的特殊性识别出特定自然人,个人信息应有助于识别出特定个人;关联指从个人到信息,如已知特定自然人,则由该特定自然人在其活动中产生的信息(如个人位置信息、个人通话记录、个人浏览记录等)即为个人信息。符合上述两种情形之一的信息,均应判定为个人信息。这也不难理解为什么匿名化处理后的信息不再属于个人信息的范畴,匿名化处理将使得个人信息主体无法被识别,且处理后不能被复原,无法从信息识别到个人。而去标识化只是在不借助额外信息的情况下,使个人信息主体无法被识别,其处理的数据仍可被还原,因此仍具有关联属性,仍属于个人信息的范畴。

需要注意的是,我国对于敏感个人信息的出境也采取了较为严格的监管措施。敏感个人信息是指一旦泄露或者非法使用,容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息,包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息,以及不满十四周岁未成年人的个人信息。相较于一般个人信息,敏感个人信息应受到更强的保护和监管。

3.其他数据

《数据出境安全评估办法》第四条规定,国家网信办规定的其他需要申报数据出境安全评估的情形,数据处理者应当通过所在地省级网信部门向国家网信办申报数据出境安全评估。而对于法律、行政法规没有特别规定的其他一般数据,例如企业一般的经营信息、商业秘密等则可以根据数据处理者的需要自由出境。

(二)我国数据出境的豁免情形

《数据跨境新规》第三条至第五条明确规定,以下几种情形可免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证:

1.国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动的特殊情形

《数据跨境新规》第三条规定,数据处理者向境外提供在国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据,如该数据中不包含个人信息或者重要

数据的,免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

2.数据过境

《数据跨境新规》第四条规定,数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供,处理过程中没有引入境内个人信息或者重要数据的,免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

3.向境外提供个人信息的特殊情形

《数据跨境新规》第五条规定,以下向境外提供个人信息的四种情形,免于申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证:

(1)为订立、履行个人作为一方当事人的合同,确需向境外提供个人信息的,如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等;

(2)按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理,确需向境外提供员工个人信息的;

(3)紧急情况下为保护自然人的生命健康和财产安全,确需向境外提供个人信息的;

(4)关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息(不含敏感个人信息)的。

对于那些数据出境情形较为简单、涉及数据量不大的企业,数据出境规定免除了它们向监管机构进行申报或备案的责任,从而显著降低了合规成本。需要注意的是,这种豁免并不意味着企业可以忽略其负有的其他数据保护义务。

(三)我国数据出境的合规路径

我国数据出境的合规路径分为数据出境安全评估、个人信息出境标准合同以及个人信息保护认证三种方式。其中,数据出境安全评估为严格的路径。如果企业落入数据出境安全评估的适用范围,那么就必须进行安全评估。而对于那些不符合数据出境安全评估标准、满足个人信息出境标准合同和个人信息保护认证的企业,可以根据自身的具体状况,自行决定采用个人信息出境标准合同或者个人信息保护认证的合规路径。

1.数据出境安全评估

数据处理者向境外提供数据,属于以下情形的,需通过所在地省级网信部门(以下简称“省级网信办”)向国家网信办申报数据出境安全评估:1)关键信息基础设施运营者向境外提供个人信息或者重要数据的;2)关键信息基础设施运营者以外的数据处理者向境外提供重要数据;3)关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供100万人以上的个人信息(不含敏感个人信息)或者1万人以上的敏感个人信息。法律规定可免于申报的情形除外。

数据处理者申报数据出境安全评估,应当通过数据出境申报系统提交申报材料。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的,采用线下方式通过所在地省级网信办向国家网信办申报。省级网信办在数据处理者提交申报材料之日起5个工作日内完成申报材料的完备性查验,并向数据处理者告知查验结果。国家网信办自收到省级网信办提交的申报材料之日起7个工作日内,确定是否受理并书面通知数据处

理者。评估完成后,国家网信办向数据处理者出具评估结果通知书。数据处理者应当按照数据出境安全管理相关法律法规和评估结果通知书的有关要求,规范相关数据出境活动。数据处理者对评估结果有异议的,可以在收到评估结果通知书15个工作日内向国家网信办申请复评,复评结果为最终结论。根据《数据出境安全评估申报指南(第二版)》,申报材料包括统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、数据出境安全评估申报书、与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件、数据出境风险自评估报告以及其他相关证明材料。

《数据出境安全评估办法》第五条要求数据处理者在申报安全评估前,应当先自行开展自评估,重点对以下事项进行评估:1)数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性;2)出境数据的规模、范围、种类、敏感程度,数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险;3)境外接收方承诺承担的责任义务,以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全;4)数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险,个人信息权益维护的渠道是否通畅等;5)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务等。

数据出境安全评估,重点就数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险进行评估,主要包括:1)数据出境目的、范围、方式等的合法性、正当性、必要性;2)境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响,境外接收方的数据保护水平是否达到我国法律、行政法规的规定和强制性国家标准的要求;3)出境数据的规模、范围、种类、敏感程度,出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险;4)数据安全和个人信息权益的保障;5)数据处理者与境外接收方之间数据安全保护责任义务的落实;6)遵守我国法律、行政法规、部门规章情况等。

由此可以看出,数据出境安全评估从出境事由是否合法正当、出境后风险对于数据处理者和境外接收方是否相对可控的维度对数据出境行为进行严格审查。其有助于识别和降低数据跨境流动的风险,从而保护国家数据安全、维护公民个人信息权益。

2.个人信息出境标准合同

《跨境新规》将个人信息出境标准合同的适用条件调整如下:1)关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供10万人以上、不满100万人个人信息(不含敏感个人信息)的;2)关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满1万人敏感个人信息的。法律规定可免于订立个人信息出境标准合同的情形除外。

根据《个人信息保护法》及《标准合同办法》,个人信息处理者向境外提供个人信息前,应当开展个人信息保护影响评估,重点评估:1)个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性;2)出境个人信息的规模、范围、种类、敏感程度,个人信息出境可能对个人信息权益带来的风险;3)境外接收方承诺承担的义务,以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全;4)个人信息出境后遭到篡改、破

坏、泄露、丢失、非法利用等的风险,个人信息权益维护的渠道是否通畅等;5)境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响等。

在进行个人信息保护影响评估之后,个人信息处理者应当与境外接收方签订个人信息出境标准合同,并履行备案义务。根据《标准合同办法》《个人信息出境标准合同备案指南(第二版)》,标准合同主要包括:第一条定义、第二条个人信息处理者的义务、第三条境外接收方的义务、第四条境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响、第五条个人信息主体的权利、第六条救济、第七条合同解除、第八条违约责任、第九条其他以及个人信息出境说明的附录。

个人信息处理者应当在标准合同生效之日起10个工作日内,通过数据出境申报系统备案,个人信息处理者备案标准合同,应当提交:统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、承诺书、标准合同、《个人信息保护影响评估报告》。省级网信办收到备案材料后在15个工作日内完成材料查验,并向符合备案要求的个人信息处理者发放备案编号。需要补充完善材料的,个人信息处理者应当在10个工作日内提交补充完善材料;逾期未补充完善材料的,可以终止本次备案程序。

如标准合同在有效期内出现以下情形之一的,个人信息处理者应当重新开展个人信息保护影响评估,补充或者重新订立标准合同,并履行相应备案手续:1)向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化,或者延长个人信息境外保存期限的;2)境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的;3)可能影响个人信息权益的其他情形。

标准合同通过约定合同义务,有效保障了个人信息的数据安全,合理兼顾了数据安全出境与数据便捷出境的需求。对于那些未达到数据出境安全评估申报标准,且不符合豁免条件仍需签订个人信息出境标准合同或需进行个人信息保护认证的出境活动,个人信息处理者可根据自身实际情况,自主选择签订个人信息出境标准合同。

3.个人信息保护认证

个人信息保护认证,是第三方专业机构对企业个人信息保护能力的认可。该认证过程严格,所需成本较高,更适合于数据规模庞大、跨境传输频繁的大型企业。

根据《个人信息保护认证实施规则》,认证流程为技术验证+现场审核+获证后监督。认证机构在对认证委托人提交的认证委托资料审查后,决定是否受理并向委托人及时反馈,受理后将确定认证方案并告知委托人。具体认证程序如下:1)技术验证:技术验证机构按照认证方案实施技术验证,并向认证机构和认证委托人出具技术验证报告;2)现场审核:在收到技术验证报告之后,认证机构将对个人信息处理者实施现场审核,并向认证委托人出具现场审核报告;3)获证后监督:根据认证委托人提交的委托资料、技术验证机构出具的技术验证报告、认证机构掌握的现场审核报告和其他相关资料信息,认证机构将进行综合评价,最终决定认证申请是否通过。对符合认证要求的个人信息处理者颁发有效期为3年的认证证书。在有效期内,认证机构将采取适当方式、以合理监督频次,对已获认证的个人信息处理者进行持续监督。认证证书有效期为3年。在有效期内,通过认证机构的获证后监督,保持认证证书的有效性。证书到期需延续使用的,认证委托人应当在有效期届满前6个月内提出认证委

托。认证机构应当采用获证后监督的方式,对符合认证要求的委托换发新证书。

在个人信息保护认证中,由于认证过程涉及第三方机构的信用支持,以及需要经历较长的认证周期和持续的监督,企业在选择这一路径时往往需要投入更多的时间和经济资源。因此,对于那些跨境业务频繁、处理大量数据的大型企业或组织来说,这种认证方式更具吸引力。一旦获得认证,它不仅能帮助企业建立良好的社会形象,还能有效增强用户对企业的信任。

三、数据出境合规建议

为了确保合规运营,我们提出以下建议供相关企业参考:

第一,企业应高度重视训练数据中重要数据和个人信息的识别工作。在数据采集、清洗和标注环节,应建立严格的筛查机制,特别关注可能涉及国家安全、公共利益的敏感行业数据。如果确认存在重要数据或个人信息,企业应当立即按照国家相关规定采取合规措施。对于难以判断的数据,建议及时与监管机构沟通或咨询专业机构,以最大程度降低法律风险。

第二,企业应根据数据来源的不同,采取相应的合规策略。对于在自身业务中直接采集的数据,如包含个人信息,企业应在采集阶段就履行充分的告知义务,并获得数据主体的明确同意。对于通过公开渠道获取的数据,由于来源复杂且难以追溯,企业应格外谨慎,尽可能确保这类数据不含任何个人信息和重要数据。而对于通过与第三方交易获得的数据,企业应在合同中明确数据出境相关条款,将合规义务转移给数据提供方,要求其保证已履行必要的合规程序。

第三,企业应当及时履行数据出境合规义务。根据出境数据的类型和个人信息的数量,企业需要判断是否需要进行数据出境安全评估、签署个人信息出境标准合同或进行个人信息保护认证。

第四,企业应建立健全的内部合规管理体系。这包括设立专门的数据合规团队,制定详细的数据出境管理制度,定期开展员工培训,提高全员合规意识。同时,企业还应建立数据分类分级制度,对不同类型的数据采取差异化的保护措施,确保数据安全。

鉴于人工智能技术的快速迭代和监管政策的不断演变,企业应保持高度警惕,持续关注国内外相关法律法规的最新动态。及时调整合规策略,以适应不断变化的监管环境。只有通过全面识别风险、严格遵守法规、建立健全内部管理体系,并保持对政策变化的敏感度,企业才能在享受技术红利的同时,有效规避法律风险,实现可持续发展。

第三篇 目标市场数据出境规则的遵循

大模型企业正以前所未有的速度拓展全球市场,凭借其强大的自然语言处理、图像识别和预测分析能力,重塑各行各业的运营模式。然而,随着数据在现代经济中的核心地位日益凸显,各国政府也越来越重视数据主权、国家安全和公民隐私保护。这导致了全球数据治理环境呈现出复杂多变的特点,给跨国经营的大模型企业带来了前所未有的挑战。本文将深入探讨大模型企业在国际化过程中如何应对目标市场的数据出境合规要求,从三个部分展开讨论:首先介绍目标市场的数据本地化存储要求,数据本地化政策作为数据出境的前提会直接影响数据出境的自由程度;其次将分析目标市场数据出境的合规要求;最后探讨企业应对目标市场数据出境监管的合规措施。

一、数据本地化存储

(一)目标市场对数据本地化存储的监管要求

大模型企业出海在目标市场进行业务运营时,应首先注意目标市场对数据本地化存储的要求。数据本地化存储是指将数据保存在其来源地区的做法。在数字经济时代,数据成为一种重要的资源和资本,因此,各国政府越来越关注数据的去向和处理方式。数据本地化存储可以确保数据在产生国的边界内被处理和存储,从而减少数据跨境流动带来的风险。数据本地化存储的实施在保护国家安全、公共利益和个人隐私方面发挥着重要作用,但同时也可能给出海企业带来合规成本和运营负担的增加。

在全球范围内,数据本地化存储的实践呈现出多样化的格局,反映了各国对数据主权、隐私保护和国家安全的不同理解和政策取向。总体而言,我们可以将全球各国对数据本地化存储的要求归纳为两种主要模式:

第一种模式是没有强制性的本地化存储要求,但对数据出境设有一定限制。例如,欧盟的《通用数据保护条例》(General Data Protection Regulation ,GDPR)允许个人数据在满足特定条件下跨境传输,如数据接收方所在国家被认定为具有充分的数据保护水平,或者采取了适当的保障措施。这种模式为企业提供了较大的灵活性,同时通过严格的合规要求确保了数据安全。

第二种模式要求数据必须首先在境内存储,但在满足特定条件后允许跨境传输和境外处理。俄罗斯的数据本地化要求就是这种模式的典型代表。俄罗斯要求企业必须确保俄罗斯公民的个人数据首先存储在俄罗斯境内的服务器上,但这并不意味着数据完全不能离开俄罗斯。在符合出境法规的情况下,数据可以被传输到境外并在境外进行处理。这种模式试图在

保护国家数据主权和允许必要的国际数据流动之间寻求平衡,为企业提供了一定的操作空间,但同时也增加了企业的合规成本。

两种模式反映了全球数据治理的复杂性和多样性。对于大模型企业而言,理解并适应这些不同的模式至关重要。企业需要根据目标市场的具体要求,调整其数据存储和处理策略。

(二)企业在目标市场实现数据存储本地化的策略

对于第一种模式,企业应主要关注数据出境相关要求。首先,企业应对数据进行详细分类,识别哪些数据属于限制出境的类别,后基于数据类别,进行全面的风险评估,确定数据处理和传输的最佳方案。其次可通过建立灵活的数据处理架构,设计能够根据不同地区要求灵活调整数据存储和处理位置的技术架构。这可能包括采用云服务提供商的区域性服务,或建立自己的分布式数据处理网络。最后,企业应对数据处理活动进行详尽的记录,包括数据流向图、处理目的说明、采取的安全措施等。这有助于向监管机构证明企业的合规性。

对于第二种模式,企业应采取相应的数据本地化存储措施。首先,考虑进行本地基础设施的部署,在目标市场建立或租用符合要求的本地数据中心,综合评估使用本地云服务提供商的可行性,建立本地数据备份和恢复系统,确保数据安全和业务连续性。其次,进行数据本地化管理,实施数据分区策略,确保相关数据首先存储在本地服务器,并确保新收集的数据默认存储在本地设施中。最后,可调整模型部署策略,使用本地模型处理初步请求,复杂任务再发送至境外模型;采取本地化模型训练方式,利用本地数据持续优化模型性能。

二、数据出境

(一)常见数据出境场景

企业还应重视目标市场有关数据出境的规则。企业在海外业务运营中涉及的数据出境场景主要有以下五种:

1. 用户数据同步与处理

企业如在中外部署服务时,用户数据往往需要在不同地区的服务器之间进行同步,以确保服务的连续性和响应速度,例如全球化社交媒体平台需要在用户旅行时,将其数据临时从居住国传输到目的地国家的服务器,以保证用户体验。再比如企业的员工协作平台需要在全中国范围内同步文档和项目数据,以支持远程工作。

2. 模型训练与优化

大模型的持续优化通常需要汇集来自不同国家用户的海量数据。这意味着各个国家和地区收集的数据可能需要传输到中央训练设施,以进行全面的模型更新。例如全球化的语音助手服务需要收集不同地区、不同口音的语音数据,以提高其语音识别的准确性,金融机构的反欺诈人工智能系统需要整合来自各个市场的交易数据,以识别新型的欺诈模式。

3. 全球业务分析与决策

为了制定全球战略和进行业务决策,企业需要对来自不同市场的数据进行综合分析,且

定期上传各类公司数据,包括但不限于员工数据、财务数据、市场数据、产品数据、技术研发数据等。这通常涉及将各个国家的运营数据传输到中国母公司。

4. 客户支持与服务改进

提供全球化的客户支持服务时,可能需要在不同国家的支持团队之间共享用户信息。此外,为了改进服务质量,用户反馈和使用数据也可能需要在全局范围内共享和分析。

5. 人力资源管理

在大模型企业的国际化进程中,人力资源管理引发的数据出境问题尤为突出,主要包括:集中化人力资源管理导致的员工信息跨境传输、全球人才招聘和调配过程中的个人数据共享、与国际服务提供商合作引起的数据传输、远程工作模式下的跨境数据访问,以及企业并购活动中的大规模数据整合。

(二)目标市场对数据出境的合规要求

不同国家和地区在数据出境监管方面呈现出多样化的特点,其监管严格程度从欧盟、中国的严格要求,到日本、新加坡的相对开放政策,各有不同。

1.相对严格的监管

以欧盟为例,欧盟的GDPR为个人数据出境设立了严格的标准,明确个人数据原则上不得向第三国或其他国际组织传输,除非通过以下三种合规路径进行:

(1)充分性认定:国家或国际组织的数据保护水平经过欧盟的认可后,个人数据即可自由地从欧盟传输至该国家或国际组织。目前获得充分性认定的国家有14个:安道尔、阿根廷、加拿大(仅适用于商业机构)、法罗群岛、根西岛、以色列、马恩岛、泽西岛、新西兰、瑞士、乌拉圭、日本、韩国以及英国。中国不在此“白名单”中。

(2)适当保护措施:当充分性认定无法实现时,数据跨境传输方则需要为欧盟境内的数据主体提供适当保障措施,具体包括:

1)公共机构之间的协议或行政安排;

2)有约束力的企业规则(Binding Corporate Rules, BCRs);适用于跨国集团企业内部数据跨境传输,要求集团在欧盟境内设有实体并获得数据监管机构对于该规则的批准。

3)欧盟委员会通过或批准的标准合同条款(Standard Contractual Clauses, SCCs);该保障措施适用最为广泛,一旦签署SCCs,数据保护的法定义务将转化为合同义务和违约责任,如果违反相关约定,则面临民事赔偿、行政处罚责任。

3)经数据监管机关批准的行为准则(Approved Codes of Conduct, CoC);该项适用于行业或部门内部进行数据跨境传输。行为准则需由代表控制者或处理者类别的协会或其他机构编制,应当包括基本原则、权利和义务、在特定传输场景下的保证、对跨境传输的说明、应当遵循的数据保护原则的说明、问责措施、数据保护义务的隐私工作人员、培训计划、数据保护审计机制、处理守则变更的机制等多项内容,最终经所在成员国的主管机关批准后由欧盟委员会通过颁布实施法案的形式来认可。

4)基于经批准的认证机制进行传输。该项是一种较新的传输机制。认证的对象是第三国的数据接收方,认证过程应当自愿,要基于有约束力且可执行的审查方式,要具有约束性和

可执行性的承诺,认证最终应当由经国家认可机构或主管的监管机构认证的认可机构根据认证标准进行检查而完成。

(3)特定情形下的豁免。该路径仅适用于前两种合规路径均不满足的情形,在符合以下情形之一可进行跨境数据传输:

- 1)获得数据主体的明示同意;
- 2)履行与数据主体间的合同需要;
- 3)为数据主体的利益而与其他主体缔结或履行合同的需要;
- 4)行使或抗辩法律主张;
- 5)跨境传输公共注册登记机构的部分数据以及保护数据主体或他人重大利益、公众利益的需要。

此外,如不遵守数据出境的法定要求,可能会面临高额罚款,最高可达全球年营业额的4%或2000万欧元,以较高者为准。

2. 相对开放的监管

以新加坡为例,其数据出境规则相对灵活,允许企业采取多种方式确保数据出境的合规性。新加坡的数据保护主要受到《个人数据保护法》(Personal Data Protection Act 2012, PDPA)的规范,PDPA在2020年修订了数据跨境传输的相关规定:除非根据PDPA相关要求确保接收方对传输的个人数据提供至少与PDPA同等的保护,否则不得将任何个人数据传输到新加坡以外的国家或地区。新加坡《个人数据保护条例》(Personal Data Protection Regulations 2021, PDPR)对此进行进一步要求,任何组织只有在采取适当措施,确保数据接收方受法律强制义务的约束,对传输的个人数据提供与PDPA同等的保护标准时,才能将个人数据向第三国转移。

满足以下情形之一的,接收方可以被认为负有了法律上的对个人数据的安全保护义务:

- (1)接收方受到与PDPA同等保护水平的法律管辖;
- (2)与接收方签订数据处理协议,该数据处理协议应约定接收方履行与PDPA同等的保护义务;
- (3)集团内签订约束性公司规则,要求集团内数据接收方提供不低于新加坡法的数据保护水平;
- (4)存在其他具有法律约束力的文件;
- (5)接收方取得特定的数据保护认证,包括了亚太经济合作组织跨境隐私规则(APEC Cross-Border Privacy Rules, APEC CPBR)系统的认证以及亚太经济合作组织流程隐私认可(APEC Privacy Recognition for Processors, APEC PRP)系统的认证。

若数据传输方因为种种原因而无法依赖具有法律效力的义务或特定认证,那么在以下情况发生时数据传输方将被视为已履行了传输限制义务:

- (1)相关自然人在被告知其个人数据将被输出至目的地国家并获得保护的情况后,同意了其个人数据的境外传输;
- (2)根据有关自然人与数据传输方达成的合同条款的规定,数据传输方合理且有必要将数据进行输出(包括传输至境外第三方中介机构)从而达到履行合同条款之目的,那么该自然

人在这种情况下被视作已经同意了对应个人数据的传输；

(3)传输数据的行为是出于对相关自然人的切身利益或国家利益保护所必须的,且进行数据传输方已采取了合理措施以确保接收方不会将获得的个人数据进行滥用；

(4)个人数据本身就是在传输过程中的数据；

(5)个人数据可以在新加坡的公开渠道获得。

需要注意的是,“相对开放”的监管并不意味着其忽视数据保护,而是在促进数据利用和保护个人隐私之间寻求平衡。对于大模型企业而言,相对开放的政策可能提供更大的操作空间,但企业仍需谨慎行事,确保数据处理实践符合当地法规。

三、企业应对目标市场数据出境监管的合规措施

在全球化浪潮中,大模型企业面临着复杂多变的数据出境合规环境。随着各国对数据主权和隐私保护的日益重视,企业必须采取全面而系统的合规措施来应对这些挑战。

(一)识别并评估数据出境过程中可能存在的风险

风险识别和评估是制定有效合规策略的基础。在这个过程中,企业需要全面审视其数据处理活动,深入了解数据流动的每个环节,并评估潜在的法律、技术和业务风险。

首先,企业应该进行全面的数据映射和分类。这个过程包括创建详细的数据目录,明确识别个人数据、敏感数据和关键业务数据,并绘制数据流动图,清晰展示数据在不同系统、地理位置间的流动路径。通过这种方式,企业可以全面掌握其数据资产,为后续的风险评估奠定基础。

在完成数据映射后,企业需要进行多维度的风险评估。法律风险评估是首要任务,企业需要对照各目标市场的法律要求,评估当前数据处理活动的合规性。这包括识别不同类型数据出境可能面临的法律障碍和合规要求,以及评估数据接收方所在国家/地区的数据保护水平。同时,技术风险评估也不容忽视,企业需要审查其数据传输和存储过程中的加密措施是否足够,评估访问控制机制的有效性,以及数据匿名化技术的可靠性。

除了法律和技术风险,企业还需要评估数据出境对业务运营的潜在影响。这包括分析数据本地化要求对运营成本的影响,评估跨境数据传输限制可能对服务质量和用户体验造成的影响,以及合规成本对整体业务模式的影响。此外,声誉风险也不容忽视。在当今用户隐私意识日益提高的环境中,任何数据处理不当都可能引发用户担忧,损害企业声誉。因此,企业需要评估其数据处理活动可能引发的用户隐私担忧,以及不同市场对数据保护的敏感度差异。

通过全面的风险识别和评估,企业可以清晰地了解其在数据出境过程中面临的各种挑战,为制定针对性的合规策略提供依据。

(二)建立完善的合规流程和管理机制

基于对风险的深入理解,企业需要建立一套全面而灵活的合规流程和管理机制,以确保

其数据出境活动始终符合各目标市场的法律要求。这个机制应该涵盖从数据收集到处理、传输、存储和最终删除的整个生命周期。

首先,企业需要制定全面的数据治理制度,明确规定数据收集、处理、传输和删除的规则,针对不同市场制定相应的数据本地化策略,并建立数据分类和标记机制,确保不同类型的数据得到相应级别的保护。

其次,企业需要设计严格的合规审批流程。这包括建立数据出境申请和审批机制,确保每次数据传输都经过合规评估。设立数据保护官(Data Protection Officer, DPO)或合规官来监督这些活动,可以进一步加强合规管理的有效性。同时,企业还应该建立与各国监管机构沟通的流程,及时获取政策更新并申请必要的审批。

技术保护措施是合规管理的重要组成部分。企业应该采用端到端加密技术保护数据传输过程,实施数据匿名化技术,降低个人数据识别风险,并部署数据泄露检测和预防系统。随着技术的发展,一些新兴的隐私增强技术,如联邦学习、安全多方计算等,为企业提供了在不实际传输原始数据的情况下实现跨境协作的可能性,这些技术值得企业关注和探索。

合同管理是另一个关键环节。企业需要与数据接收方签订详细的数据处理协议,明确双方责任和义务。对于欧盟等地区,可采用标准合同条款(SCCs)或约束性公司规则(BCRs)。同时,应定期审核和更新合同条款,以确保它们始终符合最新的法律要求。

内部培训和意识提升机制对于确保合规至关重要。企业应该对员工进行定期的数据保护合规培训,制定清晰的数据处理指南,确保所有员工了解其在数据保护中的责任。同时,建立内部举报机制可以鼓励员工报告潜在的数据违规行为,从而及早发现和解决问题。

持续监控和审计是维持合规性的关键。企业应该建立实时监控系统,追踪数据流动和使用情况,并定期进行内部审计,评估合规措施的有效性。聘请外部专家进行独立审计可以进一步增强合规措施的可信度。同时,企业还需要制定应急响应计划,建立数据泄露应急响应团队和流程,确保能够在法定时限内向监管机构和受影响个人报告潜在的数据安全事件。

最后,企业需要持续关注和适应监管环境的变化。这包括建立法规监控机制,及时跟踪各目标市场的政策变化,定期评估和更新内部政策和程序,确保始终符合最新的法规要求。积极参与行业协会和政策讨论,不仅可以帮助企业更好地理解 and 适应监管环境,还可以为塑造更有利的数据治理环境贡献力量。

通过建立这样一个全面而动态的合规管理体系,大模型企业可以有效管理数据出境风险,确保业务运营符合各目标市场的法律要求。合规不是一次性的任务,而是一个持续的过程。随着技术的发展和法规的变化,企业需要不断评估和调整其合规策略,以适应动态变化的全球数据治理环境。更重要的是,有效的数据出境合规不仅是避免法律风险的手段,更是建立用户信任、提升品牌价值的重要途径。通过展示对用户隐私的尊重和保护,企业可以在竞争激烈的国际市场中赢得优势,实现可持续的全球化发展。在数据驱动的时代,那些能够在合规和创新之间找到平衡的企业,将更有可能在全球市场中脱颖而出,实现长期成功。



知识产权

全球布局与保护

第六章

第一篇 全球知识产权策略与布局

一、大模型企业全球知识产权布局策略

(一) 专利布局原则与步骤

1. 专利布局原则

精准选择保护策略: 结合企业的经营策略、研发产品技术开发方向、市场竞争现状、财务允许范围以及不同区域的专利法规来决定。

灵活运用专利与商业秘密: 在某些情况下, 商业秘密可能比专利更能保护企业的核心技术和商业利益。

阶段性需求考虑: 根据企业的短期和长期目标, 分阶段进行专利布局。

2 专利布局步骤

- (1) 企业需要明确自身的创新点和技术路线, 并制定初步的专利布局计划。
- (2) 结合专利性评价, 从专利申请的角度, 明确创新技术方案的保护主题、申请的类型、申请地域、申请时间等, 形成策略性专利布局方案。
- (3) 在专利申请后, 需要定期维护和实施这些专利, 以确保其有效性和实用性。
- (4) 定期评估专利布局的效果, 并根据市场和技术的变化进行调整。

(二) 专利布局常见模式优劣分析

1. 路障式布局

路障式布局是一种常见的专利布局策略, 其主要目的是通过申请一种或多种必要的技术解决方案的专利, 阻止竞争对手使用该技术。

路障式布局优点在于: 路障式布局的申请与维护成本相对较低, 这使得企业在保护技术方面能够节省大量资金; 通过设置必要的技术解决方案的专利, 可以在一定时期内阻止竞争对手使用该技术, 从而保护企业的市场地位和技术优势。

路障式布局缺点在于: 尽管路障式布局可以阻止竞争对手使用某些技术, 但如果竞争对手的研发实力较强, 他们仍有机会通过回避设计来绕过这些障碍; 竞争对手在面对路障式布局时, 可能会在己方专利的启发下降低研发成本, 从而找到突破障碍的方法; 由于竞争对手可以通过规避设计突破障碍, 因此路障式布局的长期效果可能有限, 特别是在技术发展迅速的领域

路障式布局更适合技术领先型企业, 尤其是拥有核心技术并希望在短期内保护其市场地位的企业。例如高通公司布局了 CDMA 的基础专利, 使得无论是 WCDMA、TD-SCDMA, 还

是 CDMA2000 的 3G 通信标准,都无法绕开其基础专利这一路障型专利。再如,苹果公司针对手机及电脑触摸技术进行的专利布局,也给竞争者回避其设计设置了很大的障碍。

2.地毯式布局

地毯式专利布局是一种系统地对一项技术的每个研发步骤进行专利保护,形成类似于地毯的技术领域全覆盖的策略。

地毯式布局的优点在于:广泛的竞争禁区 and 严密的技术保护范围:地毯式布局能够形成广泛的竞争禁区 and 严密的技术保护范围,最大限度地保护企业的技术研发成果,阻止竞争对手的侵入;通过进行充分的专利挖掘,往往可以获得大量的专利,围绕某一技术主题形成牢固的专利网,从而有效地保护自己的技术,阻止竞争者进入;地毯式布局可以形成自身的技术壁垒,提高了竞争对手的突围难度。

地毯式布局的缺点在于:地毯式布局需要大量资金以及研发人力的配合,投入成本高;如果没有系统性的专利布局策略,容易演变为专利泛滥,无法发挥预期作用。

IBM 的专利布局模式就是地毯式布局的典型代表,IBM 在任何 ICT 技术类目中,专利申请的数量和质量都名列前茅,每年靠大量专利即可取得丰厚的许可转让收益

二、国际知识产权法律体系

(一)主要国家及地区知识产权法规对比

1.美国

(1)专利申请

在美国,专利申请主要通过美国专利商标局(USPTO)进行。专利申请的类型包括发明专利、实用新型专利和外观设计专利。美国专利申请有加速审查程序(Accelerated Examination)是美国专利商标局(USPTO)于 2006 年 8 月推出的一种程序,适用于发明和外观设计专利申请。申请人需要向 USPTO 递交加速审查的请求,并缴纳相应的费用。对于与环保、节能、反恐相关的发明,可以免交费用。加速审查要求申请人提前完成现有技术检索,并向 USPTO 提交相关文件。加速审查的审查周期为自申请日起 12 个月内。适用此程序的专利申请没有公开程序(自申请日或优先权日起满 18 个月公开),也没有相应的专利申请公开文献。

申请流程通常包括以下几个步骤:申请人需向 USPTO 提交申请文件并缴纳申请费,专利局在收到文件后 1 个月内决定是否受理该申请;专利局对申请文件进行形式审查,确定是否符合专利法要求。如果符合要求,则发出受理通知书;申请文件公开后,进入实质审查阶段,审查过程中可能会发出审查意见通知书,申请人需在规定时间内做出答复;如果经审查没有发现驳回理由,即发出授权通知书,申请人应当在收到通知书之日起三个月内完成登记手续。

(2)商业秘密保护

美国的商业秘密保护主要由各州法律调整,同时也有联邦法律的支持。商业秘密是指不为公众所知悉、具有商业价值并经权利人采取保密措施的技术信息或经营信息。商业秘密保

护不需要政府机关的授权、注册或登记,符合法律规定条件的商业秘密将自动受到保护。

(3)大模型可专利性

2024年7月16日,美国专利商标局(USPTO)发布了《人工智能主题资格指南》。结合该指南与美国法律体系,大模型技术方案多属于制造方法或操纵方式,不应排斥在专利保护范围之外,而是关注AI相关的权利要求是否展示了实际应用或技术改进。此外,大模型发明的新颖性、创造性和实用性审查标准均能够在既有专利制度框架内寻求解决路径。

2.欧盟

(1)专利申请

欧盟的专利申请主要通过欧洲专利局(EPO)进行。申请人可以选择直接向EPO递交申请,或者通过PCT途径进入欧洲阶段。欧洲专利申请的流程大致分为递交阶段、实质审查阶段和授权及生效阶段。整个过程从申请到授权通常需要3-5年的时间。申请人可以选择英语、法语或德语作为申请语言。此外,欧洲专利可以根据申请人的指定在EPC的缔约国生效。

(2)版权申请

欧盟的版权保护基于《欧盟版权指令》和《知识产权执法指令》,这些指令为软件和数据库提供了具体的版权立法。欧盟版权的主要特点是可以跨国家注册,只需一份申请即可在所有成员国享受保护。版权登记程序包括准备申请材料、填写申请表格、缴纳申请费用、提交申请材料、等待审批和颁发版权证书。欧盟还创建了在线版权注册框架,以实现规则一致、透明和高效的跨境管理。

(3)商业秘密

欧盟商业秘密保护法律规定主要依据《商业秘密保护指令》(欧盟第2016/943号指令),该指令于2016年6月8日由欧洲议会和欧盟委员会通过,并要求欧盟成员国在2018年6月9日之前将其转化为国内法。该指令旨在通过明确和统一有关商业秘密的非法获取、使用或披露的法律来保护创新和发展。根据《商业秘密保护指令》,商业秘密被定义为“秘密的、因为秘密性而具有商业价值的、已经采取合理措施保持其秘密性的”信息。指令为成员国立法提供了最低保护标准,但未涉及刑事制裁,仅涉及民事领域的法律救济。具体措施包括责令停止或禁止使用或者披露商业秘密,禁止生产、提供、使用侵权产品或将其投放市场,以及命令销毁所有或者部分侵权产品。指令还规定了在诉讼中保护保密信息的条款,并要求所有信息向法院披露时受到保护。欧盟在专利、版权和商业秘密保护方面制定了详细的法律框架,旨在促进创新和经济增长,同时确保知识产权的有效保护。

(4)大模型与知识产权

欧盟人工智能知识产权法规的主要内容涉及多个方面,包括专利保护、著作权法的适用、伦理准则以及对人工智能创作物的法律地位等。欧洲专利局(EPO)已经适应性修改审查指南,以回应产业界对人工智能相关发明在欧洲可专利性的关切。这包括对“任意技术手段”或“任意硬件”的判断以及对“具体的技术应用”或“具体的技术实施”的创造性判断。虽然人工智能生成的内容可能因缺乏独创性而不被认定为作品,但如果其表现形式与人类创作的作品类似,则需要从产生过程判断其是否构成作品。欧盟发布了《可信人工智能伦理准则》,提出了七条关键伦理要求,旨在提升人们对人工智能产业的信任,并确保人工智能的使用符合伦

理标准。欧盟的人工智能立法提案强调了对高风险人工智能系统的全生命周期监管,并提出了违法处罚原则。此外,欧盟还提出了分级监管的思想和合规评估要求,以规范人工智能的可信应用。

3.日本

(1)专利申请

日本的专利申请由日本特许厅(JPO)负责受理和审查。专利类型包括发明专利、实用新型专利和外观设计专利。发明专利的保护期限为20年,医药类发明和农药类发明的专利有效期可延长至25年。实用新型专利采用登记制,递交后5—7个月内准予注册,但行使权利时需要首先获得实用新型技术评价报告。任何人都可以在自日本申请日起3年内(巴黎公约途径)或自国际申请日起3年内(PCT途径)向JPO提出实审请求。申请人可以在提交实审请求的同时或者之后提出早期审查请求。通过早期审查程序可以加快审查进程,从提交审查请求到收到第一次审查意见通知书的时间平均为2.3个月。

申请流程如下:准备申请文件,包括申请表、说明书、权利要求书、摘要和附图(可选);提交申请文件至日本专利局,并在优先权日期后的12个月内提交相关文件以获得优先权;日本专利局进行形式审查和实质性审查,审查通过后授予专利权。

(2)版权申请

日本的版权保护在创作作品的那一刻自动产生,无需办理任何手续。尽管如此,进行版权登记有助于在发生侵权或申请强制执行时提供证明。

版权登记流程如下:提交申请材料,包括作品类别和保护期限等信息;日本版权审查员进行审查,审查通过后批准版权证书。

(3)商业秘密法律规定

据日本《不正当竞争防止法》第2条第6款的规定,商业秘密是指作为秘密管理的生产方法、销售方法以及其他对经营活动有用的技术上或者经营上未被公知的信息。商业秘密是指不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息。商业秘密的保护规定旨在制止侵犯商业秘密的行为,保护商业秘密权利人的合法权益,激励研发与创新。

4.德国

在德国,可申请的专利保护类型包括发明专利,实用新型及外观设计。德国发明专利依申请取得,需要通过实质审查以确定是否能授予权利。德国发明专利申请的受理和审查由德国专利商标局(DPMA)负责。只要满足新颖性、创造性、实用性三个条件,大模型相关算法、神经网络的特定计算模型、深度学习的计算机系统等等都可以申请专利。

申请人想在德国获得发明专利权,(1)可通过《巴黎公约》,要求优先权提交德国发明专利申请,提交申请的期限为自最早优先权日起12个月;(2)通过途径进入德国国家阶段,提交申请的期限为自国际申请日(要求优先权的,自最早优先权日)起30个月;(3)直接向德国专利商标局提交发明专利申请。发明专利从申请到授权,一般需要5—8年的时间,大约需要花费10—12万元人民币。申请人除了通过上述三个途径可以在德国获得发明专利权之外,还可以选择提交一件欧洲专利申请,自欧洲专利授权公告后,将在德国自动生效,无需办理生效手续

和提交译文,但有必要指定德国当地代理机构备案官方文件的接收地址,否则专利权人无法收到德国专利商标局发出的官方文件,因此带来的一切法律后果将由权利人自行承担。

中国国家知识产权局与德国专利商标局之间合作PPH项目。根据该项目指南,应申请人的请求,已被首次申请受理局(OFF)认定为可授权的专利申请可以在后续申请受理局(OSF)进入简易程序,获得加快审查。申请人必须用德语向德国专利商标局提出PPH的加快审查请求。德国专利商标局现在为所有PPH合作专利局提供了统一的申请表格。申请人需要填写该申请表格,并提交相关文件。在德国专利商标局尚未开始对申请进行审查之前,申请人可以向德国专利商标局提出PPH加快审查请求,但需满足:申请的专利至少有一项或多项由在先审查局认定为可授权的权利要求;同时请求进入PPH加快审查程序的德国申请中的所有权利要求必须与由在先审查局认定为可授权的一项或多项权利要求充分对应。德国专利商标局将基于合作局的工作结果独立进行检索和审查。

5.英国

(1)专利申请

在英国可以通过欧洲专利组织(EPO)申请专利与直接向英国知识产权局(UKIPO)申请专利,二者具有有不同。EPO和UKIPO在新颖性审查等方面标准不同;通过EPO申请专利涉及多个步骤和多个国家或地区的验证,而直接向UKIPO申请则相对集中于英国国内的程序;

通过EPO申请可能涉及更多的费用和时间,因为需要在多个国家或地区进行验证和翻译;通过EPO申请的欧洲专利可以在多达38个国家生效,而直接向UKIPO申请的专利仅在英国生效;通过EPO申请专利可以提供更广泛的保护范围,但程序更为复杂且费用较高。

UKIPO人工智能(AI)发明相关的专利申请审查指南及场景实例规定了UKIPO审查人工智能相关的发明专利申请的做法。UKIPO确认,只要人工智能发明对现有技术有技术贡献,就可以授予专利。UKIPO根据Aerotel四步法对人工智能发明专利进行了说明性示例,主要涉及排除性主题方面的问题。例如,涉及数学方法和计算机程序“本身”的发明被排除在专利保护之外。在2024年5月,UKIPO重新发布了关于人工智能发明的审查指南,以考虑Emotional Perception判决的影响。这一判决使得一些人工智能发明更容易获得专利。

(2)商业秘密

英国没有专门的商业秘密保护法律,而是通过普通法和判例法来保护商业秘密。普通法中的“不正当竞争”原则是保护商业秘密的重要依据。根据这一原则,如果一方通过不正当手段获取并使用他人的商业秘密,则可能构成不正当竞争。在商业活动中,签署保密协议(NDA)是保护商业秘密的一种常见做法。如果违反了保密协议,商业秘密的所有者可以采取法律行动。英国的商业秘密保护主要依赖于司法判决。根据司法判例商业秘密的认定标准包括:信息必须具有足够的保密性、信息必须是在有保密义务的情况下提供的、未经授权使用该信息。法院会根据公共利益测试来决定是否允许披露商业秘密。例如,根据《仲裁法》第23E、23F和23G条的规定,仲裁庭和法院可以在申请披露的情况下,根据公共利益来决定是否允许披露商业秘密。

尽管英国没有专门的商业秘密保护法律,但其在欧盟框架下也受到一定的保护。欧盟《商业秘密指令》要求成员国提供对商业秘密的保护,并且英国政府已经对拟议的英国法规作

出进一步修改以符合该指令的要求。英国在个人数据和隐私保护领域也有严格的立法和执行标准,这些法律间接地对商业秘密的保护起到了支持作用。例如,《数据保护法》和《隐私与电子通信条例》等法律法规对信息的处理和获取做出了明确规定。

6.沙特阿拉伯

在沙特申请专利保护有以下途径:(1)直接向沙特知识产权局(SPO)提交申请;(2)通过PCT国际申请指定沙特阿拉伯;(3)通过巴黎公约向沙特阿拉伯申请;(4)通过GCC途径。

沙特阿拉伯是《巴黎公约》成员方,因此中国的企业在向中国国家知识产权局提交专利申请时,可以利用这一途径。申请人可以优先权提出PCT国际申请,也可以直接提出PCT国际申请。提交申请时,需要确定国际申请日,并满足最低要求条件。PCT受理局将对受理的PCT申请文件进行形式审查。审查合格后,申请文件将分别送交世界知识产权组织国际局和国际检索单位。受理国家的专利局作为国际检索单位将对PCT专利申请进行检索,并做出国际检索报告。自国际申请日起满18个月后,国际局将公布PCT国际专利申请和国际检索单位做出的检索报告,在提交PCT国际申请时,申请人可以选择沙特阿拉伯作为指定国,并将该申请连同检索报告送交指定国的专利局。为了加快审查过程,申请人可以考虑加入沙特知识产权管理局(SAIP)与新加坡知识产权局(IPOS)合作开展的专利审查高速公路(PPH)试点计划。根据PPH试点计划,申请人无论收到何种类型的OA,都可以请求加速审查。GCC专利制度允许专利申请人通过GCC专利局在GCC成员国申请专利保护。申请人必须在六个GCC成员国中至少选择一个进行专利保护申请,并提交公证认证的文件。

(二)巴黎公约与PCT的分析选择

1.PCT协议

PCT只适用于发明和实用新型的申请。PCT允许申请人用一种规定的语言提交一套符合形式要求的申请文件,在所有PCT缔约国都具有法律效力。PCT比巴黎公约多出了18个月的时间,可以用来进一步验证市场及选择目标国。

PCT协议的优点在于PCT提供了一种标准化的国际专利申请程序,申请人可以在一个地方提交申请,采用一种语言、格式和支付方式,即可获得在多个成员国的有效专利保护。这一流程简化了专利申请的手续,减少了跨国家和地区的法律障碍;PCT允许申请人从首次申请日起,到进入国家阶段前有30个月的时间(或31个月,取决于具体国家的规定)进行规划和准备。这段时间内,申请人可以对自己的专利进行布局、修改和完善,还可以参考国际检索报告和初步审查报告来做出最佳决策;PCT申请的费用可以分批次支付,减少了企业短期内的财务压力。同时,PCT还为申请人提供了在进入国家阶段前的灵活性,允许他们根据市场情况和自身需求来调整申请策略;PCT国际阶段会进行国际检索和初步审查,为申请人提供有关现有技术的详细信息,帮助他们评估专利申请的授权前景,并据此决定是否继续或调整申请流程。

PCT协议的缺点在于:PCT申请分为国际阶段和国家阶段,每个阶段都有各自的手续和费用。这些额外的手续和潜在的费用可能增加经济负担,特别是在申请人寻求在多个国家保护专利时;虽然PCT国际阶段的检索和初步审查为国家阶段的审查提供参考,但其效力不直

接等同于国家阶段的审查结果。这可能需要额外的时间和资源来进行后续的国家阶段审查；PCT 申请不支持外观设计专利的保护形式，这可能限制了某些类型创新的保护可能性，特别是那些依赖于设计而非功能的创新；PCT 途径的专利申请周期通常较长，因为需要经过国际阶段和国家阶段两个阶段的审查。这可能会对需要快速获得专利授权的申请人造成一定的不便。

综上所述，PCT 协议为国际专利申请提供了一种高效且统一的途径，但也存在一些复杂性和限制。申请人在选择 PCT 途径时，应综合考虑自身需求、成本预算和时间安排等因素，以做出最适合的决策。

2. 巴黎公约

巴黎公约的优点在于：巴黎公约的核心之一是优先权原则，即在任一成员国内首次提交专利申请后，申请人可以在规定期限内（发明和实用新型为 12 个月，外观设计为 6 个月）在其他成员国提交后续申请，并享受首次申请的申请日作为优先权日；通过巴黎公约途径，申请人可以直接向目标国家提交专利申请，无需经过复杂的国际阶段；与 PCT 协议相比，巴黎公约途径的申请费用通常较低。特别是在申请国家较少的情况下，巴黎公约途径更具成本效益；巴黎公约的保护范围包括发明专利权、实用新型、工业品外观设计、商标权、服务标记、厂商名称、产地标记或原产地名称以及制止不正当竞争等。这为申请人提供了全面的知识产权保护。

巴黎公约的缺点在于：巴黎公约途径要求申请人在国内在先申请提出后的较短时间内（发明或实用新型为 12 个月，外观设计为 6 个月）完成进入各个目标国家的手续。这可能导致申请人面临时间紧迫的问题，难以充分准备和完善申请材料；由于各国专利制度、语言和文化的差异，申请人在向不同国家提交专利申请时，需要准备多种语言的申请文件，并适应各国的审查制度。这增加了申请的复杂性和成本；巴黎公约没有制定统一的专利审查标准，各国在审查专利申请时可能采用不同的标准和程序。这可能导致申请人在不同国家面临不同的审查结果和授权前景，增加了申请的不确定性和风险；虽然巴黎公约提供了对发明专利和实用新型的保护，但对外观设计专利的跨国保护相对有限。

企业在选择巴黎公约还是 PCT 的过程中，企业需要综合考虑自身的具体需求和战略目标。巴黎公约适合需要快速进入多个市场的中小企业。通过巴黎公约途径，企业可以在较短时间内获得多个国家或地区的专利权，节省时间和费用支出。然而，由于需要准备不同语言的多份申请文件，这一过程可能会带来较大的挑战。PCT 适合计划长期在全球范围内扩展业务的企业。PCT 途径可以延长申请时间至 30 个月或 31 个月，使企业有更多时间来验证市场并选择目标国。此外，PCT 途径可以在一定程度上缓解企业短期内的资金压力，更适用于落地国家较多的情况。

第二篇 人工智能企业出海知识产权保护体系建设与侵权案件诉讼策略

一、人工智能企业出海知识产权保护体系建设

(一)目标国家人工智能知识产权状况评估

在进行全球知识产权布局时,首先需要对目标国家的人工智能知识产权状况进行全面评估。这包括了解各国的专利法、商标法、著作权法等相关法律法规,以及这些法律在人工智能领域的具体应用情况。

(二)建立全球知识产权侵权监测

建立全球知识产权侵权监测系统是企业知识产权管理的基石。企业应构建一个覆盖全球的监测网络,借助专业的知识产权登记数据库、专利检索工具和市场监控平台,实时获取竞争对手的动态、行业专利申请趋势以及潜在的侵权行为。例如,通过监测全球专利申请情况,企业可以及时发现竞争对手的创新动向,预判潜在的侵权风险。一个完善的监测系统需要囊括以下关键组成部分:一是数据采集模块,负责从各种渠道收集相关信息,包括专利数据库、网络爬虫技术、社交媒体监控等;二是信息分析模块,算法对获取的数据进行筛选、整理和关联分析,识别可能的侵权行为;三是预警模块,基于分析结果生成预警报告,标记出潜在的侵权风险,并提供应对建议。

在监测系统的基础上,企业应制定风险评估和快速响应流程。风险评估包括对侵权的严重程度、可能的经济损失、对品牌声誉的影响等进行量化分析,帮助企业确定应对策略。快速响应流程则确保在发现潜在侵权时,能够迅速启动法律程序,如发送停止侵权通知、启动诉讼程序或采取其他法律手段。例如,企业可以设立专门的知识产权管理部门,负责协调各部门应对侵权事务,确保内部沟通的高效。同时,与专业的法律团队保持紧密合作,以便在侵权事件发生时提供及时的法律咨询和策略建议。

(三)风险评估与快速响应流程设计

在项目立项前,需要进行详细的知识产权风险分析,包括竞争对手的产品现状、专利情况、商品名称、型号和标识等。进行专利分析,识别潜在的侵权风险和技术壁垒。使用SWOT分析、PESTEL分析等方法,从战略、经济、技术和法律等多个维度进行综合评估。对重点领域研发计划所涉及的知识产权进行综合分析,尤其是技术相关的专利质量。

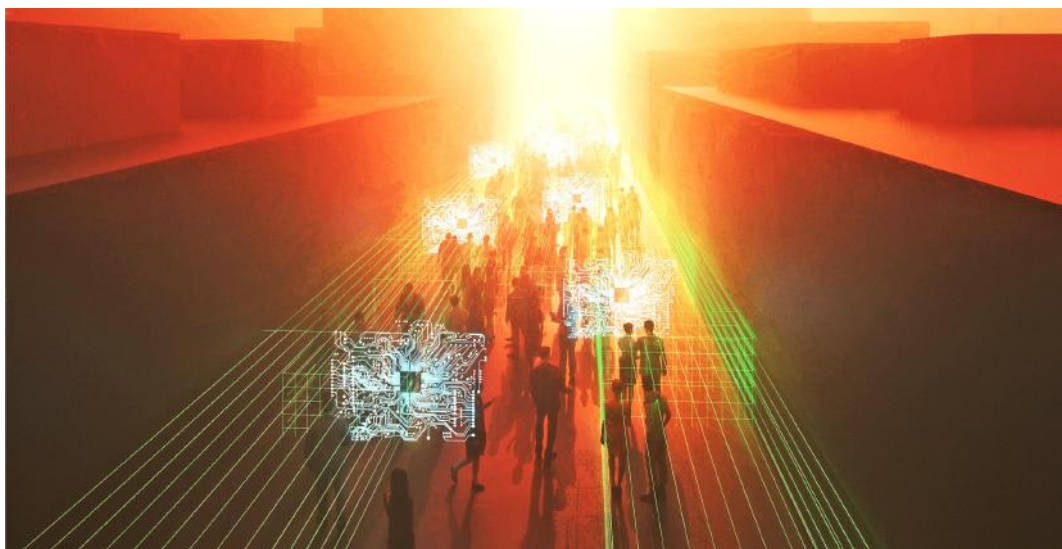
在人工智能企业出海过程中,对企业影响最大的国家或地区的知识产权法律体系主要集

中在中美和欧盟。通过运用大数据和智能化技术,可以对大量知识产权数据进行分析 and 处理,从而提高评估的科学性和便利性。例如,国家知识产权局鼓励评估服务机构开发基于知识产权大数据的智能化评估工具。使用专业的评估软件 and 数据分析工具,可以帮助评估师更系统地进行知识产权评估,确保评估过程的专业化和系统化。这些工具可以提供强大的数据处理能力 and 分析功能,帮助评估师更准确地判断知识产权的价值。在评估过程中,结合专业知识和经验进行综合分析,选择合适的评估方法,并确定相关参数的评价方法,可以提高数据知识产权价值评估的准确性和可靠性。这种方法需要充分收集技术、市场、法律等方面的信息,以保证评估结果的准确性和可靠性。积极研究推广知识产权评估相关规范与指引,发挥知识产权评估案例参考作用,提升知识产权评估的规范性和科学性。这有助于评估师在实际操作中参考成功案例,避免重复错误,提高评估的准确性。针对不同产业的特点,研发具有较高针对性的分析工具,调整评估过程中不同因素的权重,提高评估的准确性和客观度。这种个性化的方法可以根据特定行业的特征,提供更为精准的评估结果。强化科技查新能力,提升科技成果评估准确性,促进创新链、产业链、资金链、人才链的深度融合。通过科技查新,可以及时了解最新的技术趋势和竞争对手的情况,从而避免潜在风险。

针对人工智能企业的特点,设计一个有效的知识产权预警机制需要综合考虑其独特性、快速变化的技术环境以及高价值的创新成果。企业专利预警机制的核心是建立有效、可比、实用、严谨的指标体系。该体系应具有系统性、层次性和关联性等特点,并有主次和轻重缓急的区别。具体来说,可以参考以下几点:通过监测人工智能领域的最新技术动态和专利申请情况,及时发现潜在的技术突破和竞争对手的动向;分析市场需求和技术应用前景,预测未来可能产生的知识产权纠纷和侵权风险;跟踪国际和国内的知识产权法律法规变化,确保企业在合法合规的前提下进行技术创新和商业运作。

(四)法律与技术手段结合的侵权预警实践

法律与技术手段的结合,有助于提升侵权预警的精准性和效率。企业可以利用人工智能技术,如机器学习和自然语言处理,来提高知识产权信息的检索和分析能力。此外,区块链技



术可以用于记录知识产权的归属历史,为侵权诉讼提供不可篡改的证据。同时,企业可以建立内部知识图谱,将历史案例和法规信息进行整合,以便快速定位相似的侵权情况,为决策提供依据。

构建全球知识产权侵权监测系统、设计有效的风险评估和快速响应流程,以及法律与技术手段的结合,是人工智能企业实现知识产权保护的重要手段。通过这些措施,企业可以及时发现侵权行为,减少损失,并在必要时采取有力的法律行动,确保自身在全球市场中的竞争优势。

二、侵权监测要点

(一)专利侵权监测要点

企业在产品开发前进行全面的专利搜索,了解相关领域的专利状况。分析潜在的专利风险,确定是否存在侵犯他人专利权的可能性。确定所使用技术的专利是否已经过期,过期的专利技术可以自由使用。检查专利是否为开放许可,即是否可以在特定条件下免费使用。通过专利相关查询,境内外大模型企业申请专利主要是以硬件为载体承载算法总体申请专利。常见的申请组合为处理方法+实体设备。处理方法常见的有智能体的信息处理方法、文本处理方法、流量传输路径规划方法、模型训练方法、基于大模型的问答方法、数据处理方法等;实体设备常见的有存储介质、电子设备等。这些专利重点在于方法,企业应该按照权利要求书中的权利要求判定是否全面覆盖了权利要求。

(二)生成内容侵权监测要点

企业应在内容生成过程中设置过滤机制,排除可能侵犯版权的材料,监控输出内容,确保不包含受版权保护的作品的片段。企业在训练模型时应使用公共领域的数据并遵守开源许可的数据,确保所有训练数据都有合法的使用权。对于需要使用的受版权保护的材料,与版权持有人协商,确保已经获得了适当的授权或许可。企业在设计大模型时应生成原创内容,而不是复制或改编现有作品,确保生成的内容有足够的独创性,不侵犯他人的知识产权。企业确保在用户使用人工智能大模型时,明确用户协议中的知识产权条款,确定用户对其输入数据和生成内容的责任。

三、跨国知识产权诉讼策略

(一)国际诉讼管辖权选择与程序差异

在进行跨国知识产权诉讼时,选择正确的管辖法院至关重要。不同的司法管辖区可能对知识产权的保护程度、诉讼费用、审判周期和判决执行力度等方面存在显著差异。企业需要在深入了解国际司法体系的基础上,根据侵权行为的性质和发生地、自身业务布局、对方当事人

人的所在国等因素,进行周密的考量。

例如,美国是许多企业首选的诉讼地,因其在专利保护和损害赔偿方面具有较强力度,但诉讼成本高且程序复杂。欧洲各国的法律体系相对统一,但各国对版权和商标保护的执行力度可能存在差异。中国近年来在知识产权保护方面不断加强,法院的判决执行效率也得到提升,成为越来越多企业选择的诉讼地。

在选定管辖法院后,企业需要熟悉当地的诉讼程序。不同的司法管辖区可能对诉讼程序、举证责任、证据形式等方面有不同的规定。比如,美国采用“事实发现”制度,允许双方在诉讼过程中交换大量证据和信息,而欧洲的诉讼程序相对保守,更注重书面证据和法庭辩论。了解并适应这些差异能够帮助企业更有效地进行诉讼准备。

(二)证据收集与跨国取证技巧

在跨国知识产权诉讼中,由于涉及不同国家的法律和证据规则,证据的获取途径、形式和效力可能有所不同。企业需要制定有效的证据收集策略,确保证据的合法性、完整性和可靠性。企业应确保在内部建立完善的证据保存和管理机制,对可能涉及的知识产权侵权行为留有详细的记录。在跨国取证时,应遵循当地法律,避免非法获取证据,例如,未经许可进入对方服务器获取数据可能会构成犯罪。必要时,企业可以借助专业的取证团队,运用数字取证技术,如网络爬虫、数据挖掘和电子证据分析,确保证据的有效性和权威性。

企业应寻求与当地法律专家的合作,了解当地证据规则,如不同类型的证据在诉讼中的权重,以及如何有效地在法庭上呈现证据。在寻找海外证据时,可能需要通过国际合作,如双边或多边的司法协助条约,来获取对方国家的证据。同时,对于国际会议、交易会等场合产生的证据,企业应当在事前做好充分准备,确保记录的合规性。

(三)和解与仲裁:非诉讼解决机制的应用

面对跨国知识产权纠纷,企业不应仅依赖诉讼手段,还应考虑和解、调解、仲裁等非诉讼解决方式。这些方法通常能够节省时间和成本,保护商业关系,并在一定程度上维持市场稳定。

和解是通过双方协商解决纠纷,企业可以借此机会谈判达成许可协议,或者就侵权赔偿达成共识。和解协议通常具有保密性,有助于保护企业的商业秘密和品牌形象。调解则是由第三方协助双方协商,寻求解决纠纷的途径。调解相比诉讼更为灵活,且具有较强的保密性,有利于保护双方的商业关系。仲裁则是在双方同意的情况下,由独立的第三方按照仲裁规则进行裁决。仲裁程序通常比诉讼更为迅速,裁决结果往往具有约束力,且仲裁过程和结果常常可以保密。

在选择非诉讼解决方式时,企业应权衡诉讼与和解、调解、仲裁的优劣,结合案件的具体情况,选择最合适的解决方案。企业还应与专业的法律团队密切合作,确保在非诉讼解决过程中,自身权益得到最大限度的保障。

第三篇 大模型企业核心知识产权保护 路径分析与建议

一、大模型企业核心知识产权保护路径概述

(一)核心知识产权保护路径:开源抑或闭源

对于大模型企业而言,核心知识产权的保护存在两种主要的保护路径。一为通过严格完善的知识产权确权布局,将企业所有拥有的算法等智力成果置于法律强制保护的框架内,任何其他主体使用或部分使用其算法的行为,均需要获得该企业的授权,且使用需要严格限制在授权权限范围内,这种核心知识产权的保护路径即为“闭源”。另一种核心知识产权的保护路径为“开源”,通常指的是将大模型的数据信息、预训练模型权重等开放给公众,使得任何人都可以自由使用、研究、修改和分发这些模型。开源模式的核心是开源协议(亦可称之为“开源许可、开源许可证”,本文不作专门区分)。我国法律上并无“开源协议”的定义。目前国际上被广泛接受的对于“开源协议”的定义,由开源计划组织(Open Source Initiative,简称OSI)提出,即开源定义(The Open Source Definition,简称OSD)。OSD共十条标准,包括自由重新分配、源代码、衍生作品、作者源代码的完整性、不歧视个人或群体、不歧视任何领域、许可证的分发、许可不得专属于某一产品、许可不得限制其他软件、许可必须是技术中立的等十条标准,严格意义上来说,只有使用符合上述OSD全部标准的开源协议,才被视为真正的开源。开源协议的本质是附条件的著作权许可协议,是由开源软件的发布者选用的,与开源软件的被许可人约定权利义务的格式合同。

(二)影响大模型开源或闭源的决定因素

开源、闭源并无绝对的对错之分,而是企业从实际出发做出的发展战略抉择。大模型企业应当从技术保密与优势保持、社区建设与生态打造、商业利益与长远规划等角度出发,结合企业自身行业地位、客户群体、盈利模式等具体情况进行具体分析予以决策,并在企业情况发生变化时,及时调整开源或闭源策略,以适应极速的行业发展和激烈的市场竞争,实现企业的可持续发展。

1.技术保密与优势保持

对于人工智能行业乃至更为广泛的互联网企业而言,软件源代码或算法是企业赖以生存的技术基础和参与竞争的核心武器。一般来说,在大模型初创阶段,技术尚未达到领先地位的时候,大模型企业会选择开源。大模型开源建立起的社区会帮助大模型企业收集和解决大模型存在的问题,并加快大模型的迭代速度,帮助提升大模型企业的技术能力。当企业的技

术转劣为优,成为行业内的领先者时,大模型企业便可能考虑由开源策略调整为闭源策略。很多情况下,企业通过投入大量的人力、物力、财力方才构建起自身的技术优势,选择闭源的保护路径,可以有效避免核心机密的泄露,从而保持企业的核心竞争优势,凭借先发优势与迭代速率,实现行业地位的上升与巩固。

2.社区建设与生态打造

企业对大模型进行开源的最主要的考虑因素,是为打造共建社区生态,提升产品和企业自身的影响力。与闭源的模式相比,大模型开源可以汇聚起一批关注、使用本企业模型的其他主体,一方面提升业内影响力,这对于无论是用户拓展还是融资发展而言,均具有正向的作用;另一方面通过社区论坛,汇集其他主体对于模型使用的意见与建议,有助于模型算法的勘误、修正、更新,帮助企业迭代,推出更好的模型算法与产品。以腾讯、华为、百度等为代表的互联网领域大厂所推出的大模型多为闭源,原因在于这些大厂拥有成熟的产品生态和广泛的用户群体,其推出大模型一方面可以应用于现有生态的产品群,一方面可以通过现有生态推广至稳定的客户群体中,故无需通过模型开源吸引关注。而对于以智谱为代表的专门的大模型企业而言,因其并无成熟的生态社区可以倚靠,故多选择采用开源策略,从零建设社区、打造生态。

3.商业利益与长远规划

对于企业而言,采用闭源模式,可以通过知识产权使用授权许可而获得不菲的商业回报,而采用开源模式,短时间内则可能会影响商业利益的获取。但这并不是必然的。首先要区分完全开源与半开源,完全开源是指使用 OSI 认证的开源协议(“OSI-approved”)或虽未经过 OSI 认证但完全符合 OSD 标准的开源协议(“OSD-compliant”)的开源软件,而半开源则是使用自行撰写的或基于上述“OSI-approved”协议但增加诸多限制条款(如附加商业条款)的开源协议的开源软件。完全开源与半开源在商业利益方面最为明显的区别是,完全开源允许软件自由销售或赠送,不收取任何额外费用,而半开源则不然。如 Meta AI 发布的 Llama 大模型便在其第二代大模型 Llama 2 的开源协议中增加“附加商业条款”限制月活跃用户 7 亿以上的厂商使用 Llama2。该附加商业条款,并不符合 OSD 标准中规定的不歧视、不限制等标准,因此该协议属于半开源。其次,从部分企业的实践经验来看,企业可以对某个技术领域的技术进行分层,对于基础层技术实施开源,以扩大技术、产品的影响力,但对于应用层技术实施闭源保护,以保证自身核心竞争优势,或通过知识产权使用授权许可获利。如全球电动车行业领先者特斯拉,在 2014 年“前无古人”地进行专利开源,但综合来看,其系出于企业发展策略而做出的开源举措。2014 年特斯拉开源的专利共分为电池管理、电机技术、动力控制、动力回收、安全技术、充电站技术与操作系统等七个方面,均是一辆电动汽车最基础的部分,特斯拉通过开源基础专利推动行业发展的同时,掌握标准制定权,助力企业战略发展。具体来看,例如在“充电站技术”层面,特斯拉总计共有 300 余项核心专利,但处于开源状态的仅有 23 项基础层技术,后续处于应用层的 231 项核心技术则处于闭源状态,以保证特斯拉的核心竞争优势。最后,对于大模型企业而言,谨慎选择开源的技术范围,而对最为重要的部分保持闭源,亦是一种基于长远商业利益的考虑。能够支撑大模型实现模型功能的技术核心包括模型权重、数据集、源代码、训练过程和模型框架,所有的开源大模型中对上述五部分全部进行

开源的少之又少,绝大部分仅仅是对其中的一两个部分进行开源,而保持对其他部分的闭源。具有代表性的对上述几乎全部部分进行开源的大模型,如IBM开源的Granite大语言模型;更多的大模型,如智源研究院、马斯克旗下大模型公司XAI,仅开源模型权重和数据集,而对源代码等其他部分的信息保持闭源。

二、闭源大模型的知识产权布局与权利保护

(一)闭源大模型的知识产权布局

企业采用闭源路径保护大模型核心知识产权,应首先厘清大模型研发全生命周期,并针对不同周期的具体特点布局知识产权确权。应当看到,人工智能大模型与传统计算机信息软件具有软件构成上的显著差别;传统计算机信息软件主要由源代码和程序运行所需的图文音频等构成;人工智能大模型则包括数据信息(用于训练人工智能的数据集等)、用于训练和运行系统的源代码、模型参数等组成部分。数据信息并非单一模型专属使用,可以理解为大模型产品的上游原材料。关于数据信息的权属需要参考数据产权制度和数据知识产权制度,通过数据来源区分数据类型从而对号入座进行数据合规与数据确权。源代码与模型参数等可以统称为“算法”,是某一特定大模型功能实现的主要依据,即本文所谓的“核心知识产权”。

对于算法的知识产权布局保护,需要区分通过专利权、著作权和商业秘密保护的部分,并结合闭源大模型全生命周期进行知识产权保护综合布局。

1.通过专利权保护算法

国家知识产权局2019年修订的《专利审查指南》,明确了对包含算法特征的发明专利申请的审查标准。如果算法能够与技术特征相结合,整体上展现出其采用了技术手段解决技术问题,并且获得了技术效果,该解决方案便可成为专利权保护的技术方案,与普遍意义的智力活动相区别。实践中,大模型企业可就大模型智能体相关技术,申请发明专利。所谓大模型智能体,是构建于大模型之上的计算机程序,能够模拟独立思考过程,灵活调用各类工具,逐步达成预设目标的智能存在。目前,国内大模型企业正在积极布局大模型智能体相关技术的专利申请。百度作为国内领先的互联网大厂,其在大模型领域积极布局。知识产权资讯机构IPRdaily发布的中国人工智能大模型企业发明专利排行榜(TOP 50)中,百度以602件大模型专利排名第一。从国家知识产权局公布的发明专利申请书来看,百度申请的大模型相关发明专利主要包括以下几类内容:大模型硬件软件环境配置,如“大模型接口配置的推荐方法、配置、电子设备及存储介质”、“大模型插件调用方法、装置、设备及介质”;大模型搭建训练方法,如“大语言模型的更新方法和数据生成方法、装置、设备”、“大语言模型的推理方法、装置、电子设备与可读存储介质”、“大语言模型训练方法、装置、电子设备和存储介质”;大模型应用场景的解决方案,如“基于大模型的图表生成方法、装置及电子设备”、“基于大语言模型的文本处理方法与装置”、“基于大语言模型的语句生成方法、装置及电子设备”等。

2.通过著作权保护算法

计算机软件是著作权保护的“作品”,人工智能大模型是计算机软件的一种,当算法以代

码的形式成为大模型这一计算机软件的一部分时,便可以通过著作权获得保护。根据著作权保护“思想表达二分”的原则,著作权保护的是作品的具有独创性的表达,而非作品的内在思想。因此,通过著作权保护的算法,是源代码的独创性表达,而非算法内在的解决问题的思想。故如果其他人在不改变源代码思想的情况下以与源代码完全不同的表达方式进行“表达转换”,便难以达到保护算法的理想效果。但布局著作权保护,依然是知识产权保护综合布局中的重要环节。实践中,我们可通过整体软件著作权的方式,对软件源程序和计算机代码进行保护,也可通过文字作品、美术作品、视听作品等单独著作权保护的方式,对相关机器学习应用的最终呈现效果进行保护,还可对体现创造性劳动、巨额资本投入的训练集、数据集等进行数据库方面的保护。由于著作权是自动产生的,没有必须登记才能获得权利的门槛,因此著作权保护是最常见的保护方式。

3.通过商业秘密保护算法

通过商业秘密对算法进行补充保护,是业内常用的路径。商业秘密保护的范围十分广泛,算法和模型架构、训练数据和数据集、模型训练和优化技巧、硬件加速和定制化设计、软件和平台源代码等都可以作为商业秘密的保护对象。根据《中华人民共和国反不正当竞争法》的规定,商业秘密界定的构成要件包括“秘密性、价值性、相应保护措施”。作为大模型企业核心竞争力的大模型算法,通常满足以上三个构成要件:首先,大模型企业对于其大模型算法往往会采取保密措施,非授权人员无法从公开渠道获取相关资料,故算法具有保密性;其次,大模型企业为研发维护大模型算法投入巨额成本,其目的是通过大模型算法打造产品投入市场获利,或通过大模型算法使用授权获得许可费用,抑或通过大模型算法打造自营社区生态提升业内影响力,以上无论是何种目的,均符合企业运营的根本目标——营利,故算法具有价值性;最后,对于大模型算法,大模型企业会通过构建包括技术措施、管理制度在内的综合保密安全措施予以保护,故大模型算法具有相应保护措施。司法实践中,深圳市智搜信息技术有限公司诉光速蜗牛(深圳)智能有限公司侵犯商业秘密纠纷案中,深圳某法院作出的判决明确算法可作为企业商业秘密予以保护:“算法的核心是模型的选择优化,即使采用的技术都是公开模型,但如果具体模型选择和权重排序等是权利人通过大数据的收集、处理和测试后的技术成果,构成了最优选择,且不为公众所知悉,就有可能作为商业秘密予以保护。”

此处需要重点讨论的是数据窃取。数据窃取是大模型所面临的最常见威胁之一,其可分为“抽取式攻击”和“复制式攻击”两类:“抽取式攻击”是指攻击者通过访问目标模型的接口或者采用黑盒攻击的方式,向模型输入一些特定的数据,从而提取和收集特定方向的输出结果。通过大量的输入-输出操作,攻击者便可从大模型中提取出模型的结构、权重以及其他重要参数信息,而将这些数据用于新模型的训练,则很容易就可以获得与原模型相似的“全新模型”。“复制式攻击”则是指攻击者假装对大模型进行训练,获取训练过程中产生的目标模型的训练数据集或者中间结果,然后使用这些数据对自己的模型进行训练,从而获得与原模型相似的模型。经过大量的计算资源和时间的投入,攻击者甚至可以做到将原模型的数据“掏空”,直接复制出功能和性能别无二致的“双胞胎”。

大模型企业应当采取何种权利保护方式以应对数据窃取?从商业秘密的定义、认定规则来看,使用商业秘密保护方式,是应对数据窃取的有效维权手段。大模型企业应当建立健全

数据安全保密措施和管理制度,对于可能面临数据窃取的模式权重、结构等关键信息采取技术上的保密措施和制度上的保密管理,通过保密协议等方式建立起内部人员保密制度,加入数据窃取识别功能并对可能的数据窃取行为建立网络日志以便后续维权举证。

(二)闭源大模型全生命周期中的知识产权保护综合布局

为有效保护作为闭源大模型核心的算法,考虑闭源大模型全生命周期中算法形式样态的不同,企业应当考虑如下的知识产权保护综合布局:

对于尚处于原始研发阶段的大模型算法,应当通过商业秘密进行保护,要注意在企业日常运营过程中,对于“秘密性、价值性、相应保护措施”三个商业秘密构成要件的满足,以期通过商业秘密维权过程中具备充分证据与正当性基础。

对于研发完成处于维护使用阶段的大模型算法,应当综合算法的形式和保密需要予以区分保护。对于与技术特征相结合共同构成技术方案的大模型算法中,需要严格保密的部分,通过商业秘密进行保护;无需严格保密的部分,则通过发明专利进行保护。对于以独创性的源代码形式予以表现的大模型算法中,需要严格保密的部分,依然通过商业秘密进行保护;无需严格保密的部分,则通过计算机软件著作权进行保护。

(三)大模型闭源对企业权利保护与发展的影响

通过闭源大模型全生命周期中的知识产权保护综合布局,大模型企业可从多阶段、多形式、多维度对其核心竞争优势——大模型算法采取严密的保护措施,有效避免核心技术流出、导致竞争优势丧失,有助于企业在日益激烈的人工智能市场竞争中激流勇进。但应当认识到,在多家行业内领先的大模型采取开源策略、国内国外开源大模型社区层出不穷、大模型开源生态日益成熟的当下,对于大模型采取严格的闭源保护,可能会对企业业内影响力、公众满意度等方面造成较为负面的影响。



三、大模型开源策略分析与建议

(一)大模型场景下开源协议类型的选择

如前文所述,大模型开源的核心是使用开源协议,常见的开源协议包括 LGPL、Mozilla、GPL、BSD、MIT、Apache 等。这些不同的开源协议之间的差别主要体现为对某些条款采取许可、有条件许可还是限制,这些条款主要包括:商业用途、分布、修改、专利使用、私人使用、披露来源、许可和版权声明、网络使用分销、相同协议、状态变化、责任、商标使用、保修等。对于这些常见的开源协议,软件工程师阮一峰制作了下图以作区分。



注:本图版权声明为“自由转载-非商用-非衍生-保持署名”
(创意共享 3.0 许可证,即 CC BY-NC-ND 3.0)

上述这些开源协议多针对通用的计算机软件开发,主要针对源代码,而无法解决大模型开源时对于源代码、模型参数、数据信息等方面的特定要求,因此,人工智能行业内发展出专用于大模型的开源协议。与通用开源协议相比,大模型开源协议重点聚焦于大模型滥用风险的限制,在使用行为限制、商业用途等方面作出改动。最为主要的大模型开源协议包括:负责任人工智能大模型 (Responsible AI Licenses, RAIL) 系列开源协议和 Llama (Large Language Model Meta AI) 系列开源协议。

1.RAIL 系列开源协议

RAIL 系列开源协议由负责任人工智能大模型协议倡议组织 (RAIL Initiative) 发布,旨在倡导在开源协议中采用行为使用限制以降低共享人工智能技术造成的风险。RAIL 系列开源协议分支众多,最具代表性的为发布于 2023 年的 AI PUBS RAIL LICENSES。该系列开源协议,从使用用途和适用对象两个维度出发,区分为两类四种开源协议,第一类是开放的负责任的人工智能开源协议 (AI Pubs Open RAIL),具体有适用于模型的 AI Pubs Open RAIL-M 协议和适用于程序源代码的 AI Pubs Open RAIL-S 协议;第二类是仅限于研究用途的负责任的

人工智能开源协议(AI Pubs Research-Use RAIL),具体有适用于模型的AI Pubs Research-Use RAIL-M协议和适用于程序源代码的AI Pubs Research-Use RAIL-S协议。其中,AI Pubs Research-Use RAIL-M协议和AI Pubs Open RAIL-M协议的条款内容基本相同,只是将用途从开放Open(即允许下游和其他用户可以自由访问该被许可的模型)修改为仅适用于研究用途Research-Use(即仅用于学术或研究用途);AI Pubs Research-Use RAIL-S协议和AI Pubs Open RAIL-S协议的条款内容基本相同,只是将用途从开放Open(即允许下游和其他用户可以自由访问该被许可的模型)修改为仅适用于研究用途Research-Use(即仅用于学术或研究用途)。

但无论何种协议,其重点均体现在:允许免费和开放的访问、使用以及成果的下游分发,但必须始终遵守使用限制,如要求所有下游衍生作品(包括使用、修改、重新分发、重新打包)的使用都必须遵守原始开源协议中的使用限制;为防止人工智能技术不负责任地滥用而明确行为使用条款,允许开发者为特定用途授予许可,并可能限制某些用途。

2.Llama系列开源协议

Llama系列开源协议源于Meta AI公司发布的大语言模型Llama,该模型已经迭代到第三版本Llama 3。

在Llama各版本发布的同时,Meta AI公司为之定制了不同的开源协议。Llama 1协议中仅许可于研究领域,而未授予商业使用许可;Llama 2中虽然授予了商业使用许可,但增加了月活跃用户小于7亿时的特别商用条款的限制;Llama 3中与Llama 2无显著差异,主要体现在为使用方增加显著显示“Llama 3”标志的义务。

综上,大模型企业在大模型开源场景下,应当关注大模型与传统计算机软件的区别,选择大模型专用开源协议,以有效解决源代码、模型参数、数据信息等方面的开源问题。至于应当采用RAIL系列开源协议还是Llama系列开源协议,应具体参照协议的条文对许可权限、权责使用等方面的不同规定,谨慎选择。

(二)生态建设与商业利益权衡下的开源协议内容

大模型开源可增加大模型使用流量,加速大模型更新迭代,提升大模型市场影响,并通过开放社区的建设、聚集一批关注大模型发展的同道中人、打造繁荣开放的大模型生态。但,对于以营利为主要目的的企业而言,为大模型开源、开放社区建设、大模型生态打造投入的巨额成本,均着眼于长期的商业利益期待。因此,对于大模型企业而言,如何通过开源协议内容的调整,同时兼顾生态建设与商业利益,是最为重要的课题。

Llama 2开源协议中的“附加商业条款”(Additional Commercial Terms),是值得企业借鉴的成熟案例。Llama 2开源协议在Llama 1开源协议的基础上,增加了附加商业条款,内容为“如果Llama 2版本发布之日起,被许可方或其关联公司提供的产品或服务的月活跃用户数超过7亿,则其必须向Meta请求许可,Meta可能会自行决定是否授予许可,并且在Meta明确授予其此类权利之前,其无权行使本协议下的任何权利。”由于Meta在本条款中所限制的被许可方的月活跃用户数为“超过7亿”,故其目的主要为防止关键竞争对手使用Llama产品从而损害自身核心竞争利益,而非通过该条款获利。但大模型企业依然可以考虑借鉴本条

款的“熔断”机制,通过调整所需限制的被许可方的用户数量,实现通过培育大模型生态并最终获利的商业目的,同时亦可使自身的核心竞争利益得到保护。

四、大模型企业核心知识产权保护策略的建议

(一)结合企业自身实际综合采用开源闭源策略

大模型的闭源与开源并非绝对的互斥关系,企业应根据自身实际合理选择采用开源或闭源策略,并且随着具体情况的变化予以调整,以适应行业发展和市场变化。同时,或可考虑借鉴 OpenAI 的开源调整策略,在 GPT-1、GPT-2 阶段,行业发展尚不充分,大模型市场尚不活跃,GPT 技术仍存在广泛上升空间,OpenAI 选择采取开源策略,吸引更多算力、智力助力 GPT 迭代更新,推动行业成长的同时亦可提升自身行业话语权。但自 GPT3 开始,彼时 OpenAI 已成长为行业内领军企业,在技术、地位等方面均已具备绝对优势,OpenAI 又调整为闭源策略,以保证自身产品和技术的核心竞争安全。

(二)闭源策略应做好全生命周期中的知识产权保护综合布局

对于采用闭源策略的大模型技术内容,应当综合专利权、著作权和商业秘密的保护方式,根据大模型开发阶段,做好全生命周期中的知识产权保护综合布局。在大模型开发全阶段,都要做好商业秘密保护措施,方可提前化解泄密风险或为后续维权提供证据支撑;在大模型维护阶段,重点关注专利权、著作权确权工作,不仅为权利保护增加强制性排他性的权利基础,亦可作为企业授信融资的工具凭证;在权利可能遭到侵权时,要积极联系知识产权专业人员,指导内部法务部门或其他相关部门做好证据留存,有效增加胜诉概率,实现权利维护。

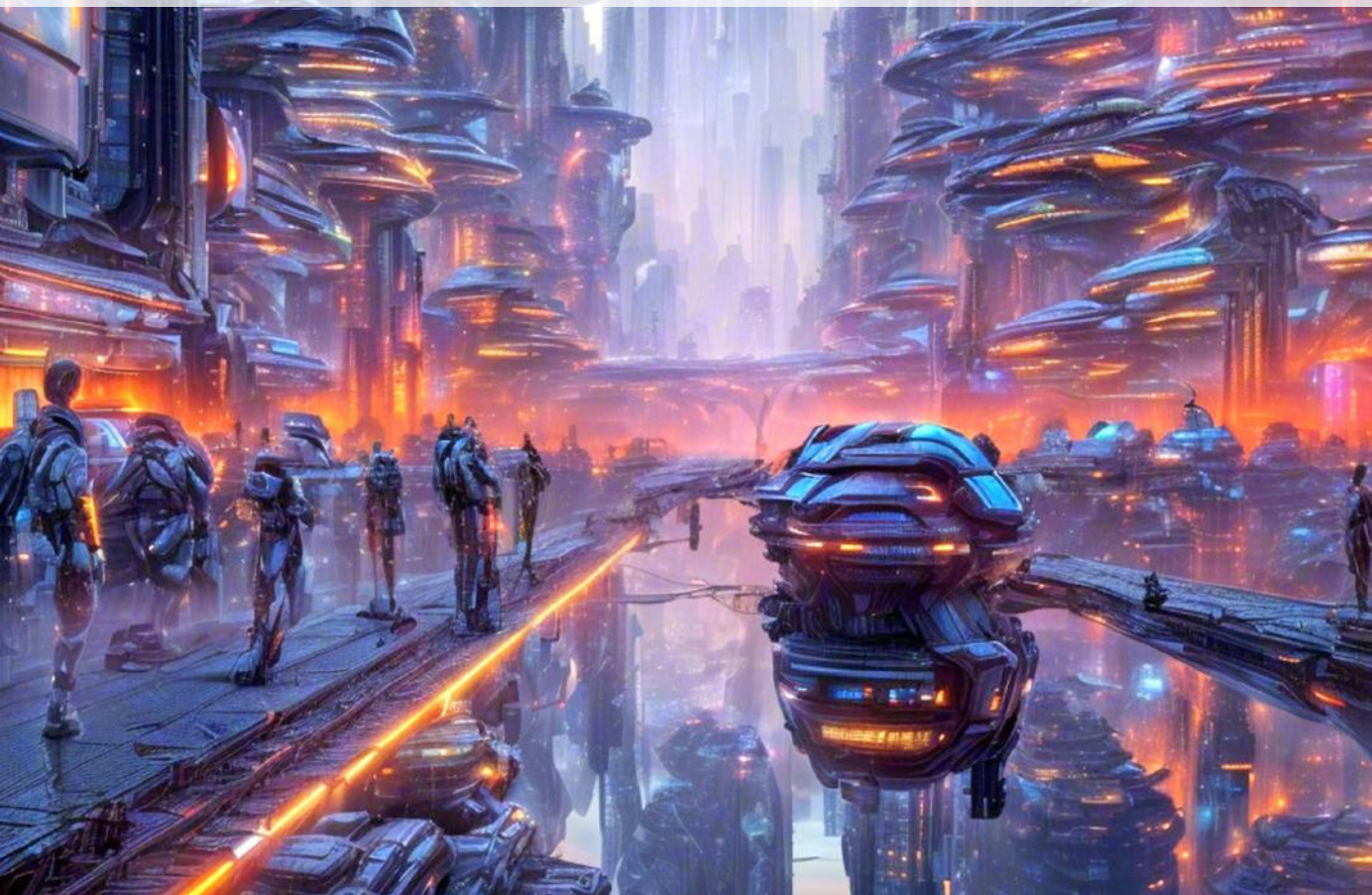
(三)开源策略应当重点关注协议选择与协议内容

对于采用开源策略的大模型技术内容,应当重点关注开源协议的选择,和生态建设与商业利益权衡下开源协议内容的调整。在开源协议选择方面,结合人工智能行业特性、大模型产品特征等,结合通用开源协议,重点基于 RAIL 系列开源协议和 Llama 系列开源协议等制定符合本企业需求的开源协议类型;选定开源协议类型后,应当综合考虑开源大模型受众、企业营利方式、企业发展战略等,重点调整开源协议中的附加商业条款,以实现企业生态建设和商业利益的双重目标。



全球化 法律支持与协作

第七章



全球化法律支持与协作

序言

在愈加严峻的市场环境下,企业的内控管理已然成为帮助企业有效控制合规风险与商务风险的重要手段。法律支持部门作为企业内控管理的核心职能部门,在风险甄别与合规监督等工作中起着至关重要的作用。对于拟开展出海业务的境内企业而言,基于全球多元法律体系的复杂性、东道国商业规则的差异性以及可分配资源的有限性,要最大限度地通过内控管理有效控制出海带来的法律风险及商务风险,必然需要建立一个高效运作、分工明确的全球化法律支持团队,以本国及东道国的法律体系为基点,通过内部统筹、外部协作的方式,为企业提供专业化、全面性的法律支持。

一、全球化法律支持部门的构建与管理

(一)团队构建

法律支持部门在大部分公司的组织架构中通常被称为“法务部”,顾名思义,是处理公司法律相关事务的职能部门。对于很多企业,尤其是业务种类较为单一、公司规模较小的企业,通常不会为法律支持部门分配较多的员额,甚至不会单设法律支持部门,仅在行政或其他后勤职能部门中配备一至两名员工来负责处理法律事务工作。这种做法容易导致公司内部决策缺乏专业支持,法律专业人员的发声空间被压缩,部门间协作困难、效率低下。据《中国企业出海专题研究报告》显示,超过60%的出海企业在初期因缺乏合规性管理而遭遇法律问题,导致业务受阻或罚款。对于拟出海的大模型企业而言,由于其主营业务涉及的法律法规及行业标准细致繁杂,加之异国投资本身面临法律风险的多样性和复杂性,组建一支配置完善、技能全面的法律支持团队将至关重要。

在确保较高的可行性和成本转化率为前提下,为保证企业的法律支持部门能够实现动静态风险控制和全过程合规管,建议企业在构建团队时,从以下两个方面进行考虑:

1.人员配置

根据企业计划出海的业务规模,参考当前业务规模下的法务团队人员配置情况及其工作量,合理构建加入出海业务后的法律支持部门的团队规模。同时,根据出海业务的需要,吸纳熟悉外商投资、知识产权、涉外劳务等国际法律实务的人才,以及具备东道国背景或资源的合规和风险管理专家,并根据工作内容设置具体岗位。

2.管理层级

确定人员配置后,企业需要对团队的管理层级进行设计。在实务中,大部分企业仍旧青睐线性垂直的管理层级划分,即由一位管理人员负责部门的整体工作,其下再进行分层管理或配置专员。拟出海大模型企业亦可以根据自身业务拓展的需要和内部管理的偏好,将出海业务与境内业务的法务工作进行隔离,建立两套平行的业务团队,并在其中分别设置垂直管理的层级。鉴于法律支持部门专业性强、独立性高,建议企业内部不设置过多的管理层级,以避免意见分散、决策不畅等不利影响。相对而言,二至三级的管理层级更具有普适性,且更易于运行和管理。

(二)专业化分工

上文已经提到,全球化的法律支持部门是由多领域的法律专业人员聚集而成的团队,每个成员均有其擅长和熟悉的业务领域,专业化分工将会帮助团队成员进一步深化各自在专业领域的职业能力,从而为公司提供更精准的法律服务。由于出海业务涉及法律事务的高度复杂性和高风险性,更需要通过专业化分工和团队协作来提高工作效率,确保法律服务质量。

企业可以根据业务种类的不同来对法律支持部门的工作人员进行分工,亦可以根据法律支持部门工作人员的专业特长来进行分工。对于大模型企业,可以参考以下团队分工设计:

- 1.AI伦理与合规团队:负责制定AI伦理指南,确保产品符合各国AI监管要求;
- 2.数据隐私团队:处理全球数据保护法规(如GDPR、CCPA)相关事务;
- 3.知识产权团队:处理专利申请、版权问题,特别是与AI生成内容相关的知识产权问题;
- 4.产品法务团队:与产品部门密切合作,处理产品设计、用户协议等法律问题;
- 5.政府关系团队:负责与各国监管机构沟通,参与AI政策制定过程。

专业化分工一方面可以将有限的人才资源集中到更能发挥效用的领域,“让专业的人做专业的事”;另一方面,可以最大限度地实现全流程、多方位、高精度的业务风险管控,确保企业在经营出海业务时更高效、更全面地适应东道国的本土法律体系,在合法合规的框架下寻求更大的商业突破。

(三)统一核心,因地制宜

作为提供专业技术支持的职能部门,法律支持部门需要保持全球法律核心策略的一致性,确保企业内部以统一的评判标准和利益导向进行决策,无论企业是否因为开展出海业务而在海外设置了独立的办公机构。因此,对于有涉外业务的企业而言,应当将法律支持部门的总体管理权收束在公司总部(或集团母公司),由总部对企业异地子公司或办事机构的法律支持部门(或法务工作人员)进行集中化管理。总部法律支持部门应主导制定核心的风险管理制度及法律事务办理程序规则,其他地区法务部门或法务人员应按照总部规定,在符合当地法律环境的前提下进行本土化贯彻落实。例如苹果公司,作为一家全球化的科技巨头企业,尽管在世界各地都有办公机构,但其始终保持着集团法律策略的一致性,尤以隐私保护和数据安全方面为甚。法律核心策略的一致性主要体现在以下方面:

1.统一的合规框架

统一的合规框架可以为企业的各个部门和海外分支机构提供清晰的行为指南,提高内部

决策效率,避免因地区差异而产生反复、冗长的沟通;

2.标准化的内部审计流程

通过实行统一的标准化内部审计,可以确保企业以相同的标准评估全球各地业务的合规性和风险状况,避免重复工作,实现资源的最优配置;

3.全球化的风险管理系统

帮助企业在全球范围内更好地识别、评估和管理法律风险,并确保法律风险和突发事件能够在企业总部决策端得到及时和统一的处理与应对。

4.统一的员工职业准则

企业可以通过对全部员工执行统一的管理制度、开展一致的员工培训,并在企业内部建立统一的员工职业准则,来促进全球员工对公司法律策略一致性的认知度和认同感。

总之,将法律核心策略的一致性融入企业内部控制体系,不仅能提高企业的运营效率和风险管理能力,还能增强其在全球市场中的竞争力和声誉。在日益复杂的国际商业环境中,保持法律核心策略的一致性已成为跨国企业成功的关键因素之一。

二、全球化法律支持部门的运作模式

一家经营出海业务的大模型产品公司的法律支持部门应采用灵活、前瞻性的运行模式。通过中央化与本地化相结合的组织结构、专业化分工、跨部门合作、全球一致的合规培训、主动参与政策制定、动态风险评估和开源合规管理等方式,法务部门可以有效管理全球法律风险,同时支持公司的创新和发展。这种模式不仅能够应对当前的法律挑战,还能为未来的监管变化做好准备,确保公司在快速发展的AI领域保持竞争优势和合规性。

(一)合规监控与风险评估

合规监控与风险评估是法律支持部门最基础且最核心的功能板块,是法务人员最需要展现专业能力与素质的工作内容,对于企业的稳健运营至关重要。

合规监控与风险评估可理解为两部分内容,一是监测管理,二为评估控制。就拟出海的大模型企业而言,法律支持部门的合规监控与风险评估工作体系可以总结为以下几部分:

1.研究制定并执行全球统一的企业合规框架

笔者已在前文“关于法律核心策略一致性”的部分强调了此项工作的重要性。对于经营出海业务的企业,法律支持部门应当在工作初期就围绕公司的核心价值取向,结合各业务经营地区的法律规定研究制定出供全球范围员工参考并遵守的合规框架。这一合规框架应至少包含:标准商务合同模板的制定、合同审批与管理、重大项目风险评估机制、定期内部合规审查机制、应急处理机制和法律培训等方面。

2.项目全周期风险评估及控制管理

为全面控制商务风险、及时提供合规建议,法律支持部门需要对企业的商务项目(包括股权投资、商务合作、资产购置等)进行全生命周期的风险评估及控制管理。具体为:在项目立项时,进行可行性分析或风险评估,必要时可以委托外部专业机构提供诸如审计、法律尽职调

查等专业服务帮助企业判断项目投前风险;在项目进行中,进行跟踪监测,承担包括项目相关商务合同审核、参与项目沟通会议、解答法律相关咨询、验证前期提出的风险规避措施落实情况等工作;在项目出现争议时第一时间启动风险应急措施,为公司提供法律意见及争议解决方案,参与争议谈判,必要时协同外部法律机构共同妥善处置争议;在项目结束后,形成结项报告,对项目最终成果、风险管理措施及落实情况、项目后续维护建议、项目经验等进行总结和归纳。

3.建立跨境数据合规体系

对于大模型企业,数据合规是必须予以重视和严守底线的合规事项。由于目前各国对于数据合规方面的管控力度存在差异,出海企业在设立内部数据合规体系时,必须考虑到各业务区域的法律差异,通过统一的底线原则搭配本地化的调整,确保全球范围内的数据传输和处理符合各国法规要求。企业可以通过开展以下工作作为实现跨境数据合规的策略:如建立全球数据地图,追踪数据流动;实施数据的本地化存储(如在业务开展的东道国设立数据中心);制定跨境数据传输协议的标准文本;定期进行数据安全评估等。

4.开展定期内部合规审计

持续的经营过程中,随着业务规模的扩大、经验的积累,以及法律法规的动态变化,企业需要不断优化和调整内部合规管理体系,以保证合规要求始终符合最新法律规定,避免因未及时更新合规措施导致不必要的损失。在此基础上,法律支持部门还应当定期在全球范围内对出海企业涉及的各地区业务进行整体的合规审计,了解各个业务区域的合规体系落实和管理现状,及时查漏补缺,持续改进合规管理效果。

全球化企业的法律支持部门在进行合规监控与风险评估时,需要采取全面、系统、持续的方法。通过建立全球合规监控体系、实施动态风险评估机制、建立跨境数据合规体系以及定期进行合规审计和评估等措施,企业可以有效管理全球法律风险,确保在复杂的国际环境中合规经营。这种全面的合规监控与风险评估方法不仅有助于企业遵守各国法律法规,还能提升企业的声誉和竞争力。在日益复杂的全球监管环境中,法律支持部门也需要不断创新和改



进其合规管理方法,以应对新的挑战和风险。

(二)内部培训与知识共享

前文“全球化法律支持部门的构建与管理”这一章节中已经提到,对于经营出海业务的企业而言,其法律支持部门的团队成员往往有着各自不同的专业背景,并依其擅长方向的差异在部门中承担着不同的分工。在此背景下,法律支持部门通过建立内部培训制度来促进团队内乃至企业整体知识分享和经验传递的必要性不言而喻。

企业可以通过开展以下内部培训活动来提升法律支持部门成员的综合能力、加强企业合规的可持续发展:

1.建设全球统一的培训平台

以通用电气作为参考,企业可以建立一个向全球员工开放的统一在线学习平台,其中包含法律和内部合规培训,帮助各个地区的员工都能获得一致的法律知识。企业可以开发针对不同职级和部门的定制化法律培训课程,也可以利用AI技术提供个性化学习路径,吸引员工的学习欲望,提高学习效果。

2.建立跨区域法律知识库

以IBM(International Business Machines Corporation,即国际商业机器公司)的Watson法律助手作为参考,企业可以利用其AI技术开发内部法律知识管理系统,创建包括法规解读、案例分析、合同模板等内容的结构化知识库,帮助全球法律支持团队成员快速检索和应用相关法律知识;同时还可以建立贡献激励机制,鼓励全球团队成员在该知识管理系统中积极分享本地知识,丰富知识库内容。

3.开展法规适应性培训

欧盟《一般数据保护条例》(“GDPR”)第39条中要求数据保护官(“DPO”)接受持续的专业培训,这一要求可以扩展到企业的整个法律支持团队。比如企业可以针对不同地区的特定法规(如GDPR、《2018年加州消费者隐私法案》(CCPA)、《中华人民共和国个人信息保护法》(PIPL)等开发专门培训模块,或与当地监管机构合作开发培训课程,确保培训内容符合最新监管要求。

4.召开案例研究分享会或法律研讨会

企业可以定期召开案例研究分享会或法律研讨会,以行业内热点案例或公司实际发生的案例为切入点,围绕数个核心法律问题,汇集全球法律支持团队成员共同研究讨论,分享各自的实务经验和心得体会,同时也可以邀请外部专家共同参与头脑风暴,以求解决实际的法律问题。

通过以上方法,企业的全球化法律支持部门可以有效进行知识共享,确保全球团队保持高水平的法律专业知识,同时适应不同地区的法律环境。除此之外,这种全面的培训和知识共享体系还可以提高法务团队的协作能力,促进企业整体的法律风险管理水平,提高企业的竞争力,支持企业在全球市场的可持续发展。

(三)危机管理与应急响应

在全球化经济背景下,出海企业面临着日益复杂的法律环境和多元化的风险挑战。从产品安全危机到数据泄露事件,从供应链中断到反垄断调查,企业需要应对的危机类型日益多样化和国际化。在这种背景下,全球化企业法律支持部门的角色和职能正在发生深刻变化,从传统的被动防御转向主动预防和全面管理。在此背景下,企业建立起全方位、前瞻性的法律危机管理不仅能够降低企业的法律风险和声誉损失,还能增强企业的全球竞争力。

1.建立全球统一的危机应急响应机制

企业应当建立统一的危机应急响应机制,在出现法律风险事件的第一时间启动。法律支持部门应当在应急响应环节承担主导地位,统筹其他如商务、公关、运营等相关部门员工共同建立危机处理团队,确保在处理危机事件时的信息共享和行动一致。统一的危机响应机制能确保企业在不同地区都能快速、一致地应对危机,降低法律风险和声誉损失。

2.跨境数据泄露应对

在互联网科技高度发达的今天,对于大模型企业,数据泄露风险是易发的高风险项目,也是企业危机管理的重中之重。法律支持部门在应对数据泄露风险事件时,需要充分利用其对于各国相关法律法规的掌握,在企业技术手段之外,通过法律手段尽可能进一步降低相关事件带来的不利影响,减少潜在的罚款和诉讼风险。比如法律支持部门可以根据当地法律要求执行相应的跨国数据泄露通知流程,确保符合各国法律要求的时限和内容;与各国数据保护机构积极沟通,协调参与调查程序,并提供必要的法律支持;制定全球统一的数据泄露应对策略,包括数据恢复、安全加强和赔偿方案。

全球化法律支持部门在危机管理与应急响应工作中的作用主要体现在统一策略、风险管控、跨境协调、长期预防等方面。通过这些工作,全球化法律支持部门不仅能够帮助企业有效应对即时危机,还能提升企业的整体风险管理能力,为企业的可持续发展提供强有力的法律保障。在日益复杂的全球商业环境中,这种能力已成为跨国企业核心竞争力的重要组成部分。

三、法律支持部门面临的全球化管理挑战

全球经济一体化的发展使出海企业的海外经营不断深化,企业对法律支持部门的期望也在不断变化。在全球化背景下,法律支持部门对公司运营的影响越来越大,其所面临的挑战也越发多样。

(一)跨境合规适应性的挑战

AI技术的快速发展往往超过了现有法律法规的适应能力,导致了各国监管政策的不一致性。大模型企业在全域运营时面临的一个主要挑战是如何在不同的法律框架下保持合规。除却通过前文提到的建立全球统一的企业合规框架来保证跨境的合规适应性外,法律支持部门还可以通过以下方式应对和化解不同法律环境下的合规挑战。

1.建立全球合规矩阵

通过创建一个动态的合规数据库整合各国人工智能及数据保护领域的相关法律法规,并

对其差异之处进行归纳总结,方便全球法律支持团队的成员进行查阅学习。同时,可以利用AI技术动态追踪全球法规的变化,及时更新合规矩阵。此外,法律支持部门也应当定期召开跨区域法律事务沟通会议,分享各自业务区域内的热点事件和最新法规,讨论合规矩阵的更新和应用。

2.配合监管、主动合规

企业各业务区域的法律支持部门可以平行成立专门的政策参与团队,寻找机会积极、主动参与各国AI政策的制定过程。此外,还可以组织或赞助AI相关的产业峰会或学术研讨会,影响当地行业标准的形成。法律支持部门还应当保持与当地监管机构的良好关系,建立起有效的沟通协调机制,降低企业因合规适应性瑕疵可能产生的行政风险。

(二)应对文化差异的挑战

对于大模型产品而言,AI产品输出的结果在不同的文化背景下可能产生意想不到的效果,这使得文化差异也成了一项极大的挑战。语言习惯、社会规范、道德观念的差异可能导致AI输出不当或具有冒犯性的内容,从而引发危机事件;同时,企业与合作伙伴之间的任何文化差异都可能导致企业内部产生不同的理解或沟通困难,从而影响公司业务的开展。在此情形下,跨文化沟通和协作能力对法律支持部门而言是一项重要的工作内容。

为有效应对此项挑战,法律支持部门可以采取以下措施:

1.多元化团队建设

吸纳当地人才进入法律支持团队,通过专业分工、知识共享和协作互通,改进团队的文化多样性、增进团队成员对不同文化的理解。

2.创建跨文化合作项目

在跨文化沟通中,鼓励不同文化背景的团队成员共同解决问题,互相倾听、多重探索,以企业共同的价值取向为原则,求同存异,帮助企业选择最优的路线。

3.文化适应性专项训练

法律支持部门应当收集、研究相关资料,或与当地文化机构合作,获取对特定文化禁忌和敏感话题的专业意见,制作形成文化敏感性培训课程或备忘录,提供给技术部门用于开发针



对AI特定内容风险的训练策略。同时也应配合建立AI输出的多层次审查机制(包括自动化检查和人工复核),将内容审核包含在其中,及时捕捉和解决涉及内容风险相关问题。

(三)商业模式的差异与适应

商业模式是指企业运营的具体方式。不同的商业模式,会导致企业在合规方面、劳动用工方面、销售流程方面、财务方面等都会有差异。比如,在美国,许多企业都建立了自己的合规部门。而在英国,公司可能更多地通过聘请一家欧洲合法经营且业务范围广泛的外国律师事务所来提供专业的法律顾问服务。这些差异可能会影响到企业的法律支持部门,使其在处理各种合规问题时,需要有相应的应对策略。

1.建立灵活的法律框架

通过设计灵活的商务合同模板,包含适用于不同商业模式的法律结构模板,以快速适应不同市场的需求。

2.建立跨部门的商业模式评估团队

在每次开展新业务或开拓新地区市场前,汇聚包括法律支持、财务、商务、运营、人事等部门的代表成员,组建一支跨部门的商业模式评估团队,对开拓新业务或新市场的综合风险进行评估,并预测不同商业模式对业务的影响,从而做到对不同业务模式的风险程度有所预期,有所防范。

3.定期商业模式法律审查

通过对各市场业务的合规风险开展定期评估,审查全球各地的商业实践效果,及时发现和响应可能影响商业模式的法律变化。

(四)公共关系的搭建与维护

大模型企业需要在全球范围内管理公众对AI的期望和担忧,包括处理隐私 concerns、就业影响、AI伦理等敏感话题,同时还要适应不同国家的政治和社会环境。由于政府和其他利益相关者可能会对企业进行施压,因此企业必须建立起有效的公共关系来应对这些风险。在这种情况下,企业的公共关系部门需要综合把控和管理相关的公关风险,帮助企业协调政府关系、配合监管问询等,而法律支持部门也需要提供一定的协助工作。

1.法律文件审核

在与政府或监管机关合作时,企业可能会与之签署一些具有法律效应的文件和合同,法律支持部门需要配合公共关系部门按照与政府或监管机关达成的一致意见审核对应的法律文件,保障企业的合法权益。

2.参与可行性分析

法律支持部门应会同公共关系部门共同对拟开展的公共关系活动进行可行性分析,具体考虑该活动:①是否符合公司的品牌战略;②是否能充分反映公司文化和价值观;③是否对公司有益;④是否具有吸引力;⑤是否具有可持续性等。

3.其他配合工作

法律支持部门应该为员工提供相应的培训和指导,以帮助员工正确应对客户、合作伙伴

以及媒体等的询问;另外,还应当主动采取措施,与外聘律师、专家等外部资源建立良好关系,以实现相互支持、互相协作。

未来,随着技术的发展和全球经济格局的变化,出海企业的法律支持部门将面临更多、更新的挑战和机遇,人工智能、大数据等技术的应用可能会改变法律支持的方式和效率,持续学习和适应能力将成为法律支持团队的核心竞争力,使他们能够在快速变化的全球AI监管环境中为企业提供有效的法律支持和战略指导;另外,新兴市场的崛起和国际贸易环境的变化也将要求法律支持部门具备更加全面和前瞻性的视野。与此同时,企业也应当持续强化法律支持部门的战略地位,投资于人才培养和技术创新,以应对未来可能出现的复杂危机。

四、外部法律服务机构的选择与有效利用

中国企业在走向世界的过程中,既面临着越发激烈的市场竞争,同时也要面对很多不确定的法律风险。而外部法律服务机构作为一个汇聚专业人员的服务机构,是中国企业在海外投资过程中不可或缺的重要资源。面对市场上琳琅满目的备选机构,如何选择一家优秀的外部法律服务机构并有效利用其服务来增益自身对于企业来说至关重要。

(一)明确合作目标和期望

大模型企业面临的法律挑战往往涉及新兴技术领域,需要具备专业知识和前瞻性思维的合作伙伴。相较于外部机构的规模和人数,更为重要的是它的专业度和适配度。明确合作目标和期望是选择合适的外部法律服务机构的基础,企业应当以战略性和系统化的眼光对备选机构进行综合的评估,以确定最为适配的服务团队。

1.建立量化评估矩阵

法律支持部门作为和外部法律服务机构对接的第一责任部门,应当创建一个详细的、量化的评估矩阵,包括专业知识、行业资历、既往案例、海外资源等关键指标,也可以为不同类型的法律事务(如知识产权、数据合规、争议解决等)设置不同的评估权重。之后,与备选服务机构进行过充分讨论,并查阅、分析了对方提供的材料后,结合企业自身的合作需求和预期目标,以该评估矩阵为指导,对备选服务机构进行评分,择优选定。

2.多机构协同服务

不同的外部法律服务机构其专长和经验不同,各自擅长的领域也不同。因此,企业需要将这些外部法律服务机构的专业特长与企业自身的战略目标结合起来进行研究,针对不同的合作目标选择不同的服务机构。例如,企业可以选择两个外部法律服务机构分别提供常年法律顾问服务和数据合规专项法律服务。

3.定制化绩效考核与定期合作审查

企业在寻求外部法律服务机构帮助时,需要了解律师团队是否具备跨专业领域的法律技能,是否能根据项目需要快速组建团队并进行有效管理,而验证合作效果最便捷最公允的方式便是通过设定定制化的绩效目标对其进行考核。当然,基于企业自身需求和现状的不同,法律服务成果存在部分难以量化和完成度存在客观性障碍的特点,企业可以同步通过制定明

确的短期和长期合作目标(包括具体的关键绩效指标)作为考核依据。同时,企业应当建立定期的合作审查机制,评估合作目标的达成情况,如以季度或年度为单位对外部法律服务机构在审查周期内的工作表现进行整体的审核与确认,并依审查结果调整合作策略和期望。

(二)建立高效的沟通与协作平台

中国企业在开展出海业务的过程中,往往存在着法律服务资源分散、服务效率低下、沟通和协作困难的问题。有效的沟通和协作对于大模型企业与外部法律服务机构的合作至关重要,尤其是在处理跨境和技术密集型案件之时。例如,微软开发了一个名为“Legal Workload Management Solution”的内部平台,用于管理和协调其全球法律工作,其中就包括了与外部法律服务机构的合作对接。

企业可以通过以下方式构建一个高效、即时的协作体系:

1.建立集成化协作平台

邀请外部律师使用与企业相同的办公协同平台,集成文档管理、即时会话、线上会议、工作进度跟踪等功能,方便将外部法律服务机构纳入公司的整体管理体系中。这一办公协同平台应当具备强大的安全和隐私保护功能,以保护企业的敏感信息。

2.优化沟通与反馈机制

毫无疑问,企业期望外部法律服务机构能够做到有问必答、及时响应。要达成这一目标,需要企业与外部法律服务人员一同对双方的沟通与反馈机制不断优化。企业应坦率提出自己的需求,主导与外部机构定期组织线上会议和视频通话、确定项目反馈的时效要求与频率要求,确保双方信息交流及时,避免因双方之间存在信息差导致的效率低下。

(三)成本效益与服务质量控制

企业在选择外部法律服务机构时,既要确保法律服务的高质量,同时也要控制相关成本支出。往往需要综合考虑经济、效率和风险三个方面的因素,才能锁定心仪的外部法律服务机构。

与外部法律服务机构合作虽然必然增加企业的成本支出,但通过以下方式亦可以在有限的成本支出范围内,获取更高的服务质量和收益:

1.智能化费用管理

企业可以通过建立动态定价模型,根据需求复杂度、实现难易度和最终增益价值等因素调整费率,合理控制服务费用的支出;同时可以对不同类型的法律事务采用不同的收费模式,探索创新的收费模式,如固定费用、上限费用或基于结果的收费等,优化成本结构。

2.内外部资源平衡

任何一家外部法律服务机构都无法解决所有问题。企业可以建立清晰的指导原则,将相对重复性较高、专业度一般且外部依赖性低的事项交由内部法律支持部门自行处理,将特异性强、专业度和难度双高事项交由外部机构承办。在合作过程中,企业应当定期评估内部法律事务处置能力建设的成本效益,进一步优化资源配置,减少支出。

3.建立服务质量评估体系

企业可以开发多维度的服务质量评估体系,对外部法律服务机构的服务专业度、目标完成度、服务响应速度、思维创新性等指标进行评估,并将评估结果与费用支付比例挂钩。企业也可以通过对外部机构开展定制化绩效考核与定期合作审查,将结果与续约和奖励机制挂钩,保证费用支出的合理性。

(四)知识与经验的积累转移

与外部法律服务机构的合作不仅是为了解决当前的法律问题,更是获取专业知识和经验的机会。知识与经验的积累转移是一个双向的过程,这就要求企业在选择外部法律服务机构时要考虑到如何对合作伙伴进行有效利用。

首先,企业在选择外部法律服务机构时,要考虑其是否有相应的培训计划,以便为合作伙伴提供相关的培训,从而使得合作伙伴能够获得专业知识与技能方面的支持。其次,企业要考虑外部法律服务机构是否拥有足够的内部资源以供自身使用。企业可以通过与外部法律服务机构签订战略合作协议,来保证双方能够充分利用彼此资源。最后,企业可以将知识分享活动纳入外部法律服务机构的绩效考核目标,与服务费用挂钩,以提高其服务积极性。

企业内部与外部法律服务机构的知识共享与经验积累可以通过以下方式实现:

1.建立知识共享系统

在企业内部创建共享的知识库,向合作的外部法律服务人员开放访问权限,允许其查阅其中资料,同时鼓励其参与贡献知识资源。

2.制定知识转移计划

通过制定结构化的知识转移计划,要求外部法律服务机构定期提供法律培训或作为主讲人参加知识分享会。另外,企业可以安排法律支持部门的工作人员作为与外部法律服务人员的指定对接人,成为其团队的“影子成员”,跟随学习。

3.案例积累和实践记录

企业可以会同外部法律服务机构将合作过程中办理的法律事务整理记录,并汇总为案例库或法律事务实践指南,将外部合作中获得的洞见纳入公司政策和流程。

结 语

在全球化的大潮中,大模型企业出海已成为不可逆转的趋势。面对复杂多变的国际法律环境,企业法律支持部门的角色愈发重要。法律支持部门不仅需要应对传统法律事务,还应在AI伦理、数据隐私、知识产权等新兴领域中发挥关键作用。在AI技术日新月异的今天,法律支持部门不仅是企业合规的守护者,更应成为企业创新的推动者,为企业的创新发展提供法律支持和战略指导。

未来,随着技术的发展和全球经济格局的变化,法律支持部门将面临更多新的挑战 and 机遇。企业必须持续强化法律支持部门的战略地位,投资于人才培养和技术创新,以应对未来可能出现的复杂危机。唯有如此,企业方能在全球市场中立于不败之地,实现可持续发展。



出口管制 与合规

第八章

第一篇 人工智能技术出口管制与应对策略

一、我国对外贸易管制概述

我国企业对外出口人工智能技术将会涉及对外贸易管制合规问题。目前,我国对外贸易管制体系包括三项制度,分别是出口管制制度、技术进出口禁限管理制度以及不可靠实体清单制度。

(一)出口管制制度

为维护国家安全和利益,履行防扩散等国际义务,我国通过《中华人民共和国出口管制法》及其他相关法律法规建立起依法出口管制制度。出口管制制度的主要管制对象为两用物项、军品、核以及其他与维护国家安全和利益、履行防扩散等国际义务相关的货物、技术、服务等物项。参照最新版本的《两用物项和技术进出口许可证管理目录》和《军品出口管理清单》中的具体物项、技术清单,人工智能技术尚未被列入其中,但不排除未来被列入的可能性。

(二)技术进出口禁限管理制度

1.技术进出口禁限管理制度的规则体系

技术进出口禁限管理制度体系主要是以《中华人民共和国对外贸易法》(以下简称:《对外贸易法》)第16条为核心,辅以相关法规规章建立的。该制度的建立旨在规范技术进出口管理,维护技术进出口秩序,促进国民经济和社会发展。制度的主要法律法规构成除上述《对外贸易法》外,还包括《中华人民共和国技术进出口管理条例》(以下简称:《进出口管理条例》)《禁止出口限制出口技术管理办法》《中国禁止出口限制出口技术目录》(以下简称:《出口目录》)《技术进出口合同登记管理办法》(以下简称:《合同登记办法》)等。

根据该制度体系,技术的出口被分为自由出口技术、限制出口技术和禁止出口技术。其中,属于禁止出口技术的,不得出口;属于限制出口技术的,实行许可证管理,未经许可的,不得出口。商务部会同科技部按照《对外贸易法》第16条标准确定具体的禁限技术目录并适时调整。

2.人工智能技术出口管理制度的管辖范围

《进出口管理条例》第二条规定了技术进出口禁限管理制度的管辖范围:技术出口行为指的是从中国境内向中国境外,通过贸易、投资或者经济技术合作的方式转移技术的行为。技术出口的管辖为属地管辖,重点关注技术产生地,而非技术权利人国籍。技术出口的形式包括专利权转让、专利申请权转让、专利实施许可、技术秘密转让、技术服务和其他方式的技术转移。其中“其他方式的技术转移”涵盖范围十分广泛,几乎可以涵盖以任何形式向其他个人

或组织披露和传播技术信息。这包括正式的技术提供行为,如提供数据接口;也包括非正式的技术提供行为,如电子邮件。同时需要注意,跨国公司的国内机构与国外机构之间的内部技术交流,也存在被认定为技术进出口行为的可能。

3.人工智能技术出口法律责任

企业违法出口禁止或者限制出口的技术,根据《进出口管理条例》第43条和第44条规定,其需要承担行政责任,如没收违法所得、罚款、撤销对外贸易经营许可等;情节严重构成犯罪的,则需要依照走私罪、非法经营罪、泄露国家秘密罪等规定依法追究刑事责任。

(三)不可靠实体清单制度

为了维护公平、自由的国际经贸秩序,维护国家主权、安全、发展利益,保护我国企业、其他组织或者个人的合法权益,我国通过《不可靠实体清单规定》建立不可靠实体清单制度。该制度的规制对象为符合一定标准的外国实体,包括外国企业、其他组织或者个人。目前公布的不可靠实体共计五家,同时还有一家风险企业。我国企业在进出口经营活动中不得与实体清单企业开展相关进出口活动,特殊情况下确需开展交易的,需向不可靠实体清单工作机制办公室申请,经同意方可进行。目前的不可靠实体均非主要的人工智能企业,但我国企业仍需进行必要的尽职调查,避免承担法律责任。

二、人工智能技术出口的分类规制

(一)人工智能技术出口规制分类

如前所述,技术的出口分为自由出口技术、限制出口技术和禁止出口技术。自由出口技术指的是不在《出口目录》禁止出口和限制出口范围的技术;限制出口技术指的是《出口目录》所列限制出口的技术;禁止出口技术是《出口目录》所列禁止出口的技术。《出口目录》中涉及的与人工智能相关的技术,基本上均归为限制出口技术。以上三类技术的出口流程有所差异。

(二)自由出口人工智能技术的范围及出口流程

人工智能技术是否属于自由出口技术,应采取排除法判断。不在《出口目录》内的人工智能技术,即可自由出口。自由出口人工智能技术,需要进行合同登记。

根据《合同登记办法》,国家对自由进出口技术合同实行网上在线登记管理。拟出口企业应在商务部网站上的“技术进出口合同信息管理系统”中进行合同登记,并持技术出口合同登记申请书、技术出口合同副本(包括中文译本)和签约双方法律地位的证明文件,到商务主管部门履行登记手续。商务主管部门在收到上述文件起3个工作日内,对合同登记内容进行核对并颁发《技术出口合同登记证》。

上述合同登记的主要内容包括:合同号、合同名称、技术供方、技术受方、技术使用方、合同概况、合同金额、支付方式、合同有效期。

(三)限制出口人工智能技术的范围及出口流程

《出口目录》所列的人工智能技术,被归类为“软件和信息技术服务业”领域中的“信息处理技术”分类项下。主要包括:智能汉字语音开发工具技术、中文平台技术(中文处理核心基础)、中译外翻译技术(机器翻译系统得分>4.5分,满分为5分)、少数民族语言处理技术、专门用于汉语及少数民族语言的语音识别技术、印刷体汉字识别技术、程序结构、主要算法和源程序、Videotex(可视图文)系统的汉字处理技术及网间控制技术、具有交互和自学习功能的脱机手写汉字识别系统及方法、用于计算机汉字输入识别方法中的手写体样张、印刷体样张以及汉语语料库、汉字识别的特征抽取方法和实现文本切分技术的源程序、专门用于汉语及少数民族语言的语音合成技术、专门用于汉语及少数民族语言的人工智能交互界面技术、专门用于汉语及少数民族语言的智能阅卷技术、基于数据分析的个性化信息推送服务技术(基于海量数据持续训练优化的用户个性化偏好学习技术、用户个性化偏好实时感知技术、信息内容特征建模技术、用户偏好与信息内容匹配分析技术、用于支撑推荐算法的大规模分布式实时计算技术等)。

对于以上限制出口的人工智能技术的出口,应当获得出口许可。出口许可申请的具体流程如下:

1.向地方商务主管部门提出技术出口申请:

在对外进行实质性谈判、作出有关技术出口的具有法律效力的承诺前,向地方商务主管部门提交《中国限制出口技术申请书》。属于国家秘密技术的限制出口技术,在技术出口申请前,应先按《国家秘密技术出口审查规定》办理保密审查手续,获得保密审查主管部门批准的《国家秘密技术出口保密审查批准书》后方可进行技术出口申请。

地方商务主管部门自收到《申请书》之日起30个工作日内,会同地方科技行政主管部门分别对技术出口项目进行贸易审查和技术审查,并决定是否准予出口。地方商务主管部门应在收到《申请书》之日起5个工作日之内,将相关材料转地方科技行政主管部门。地方科技行政主管部门在收到《申请书》之日起15个工作日内,组织专家对申请出口的技术进行技术审查并将审查结果反馈地方商务主管部门,同时报科技部备案。

2.获得有效期为3年的《技术出口许可意向书》:

出口申请获得批准后,由地方商务主管部门颁发由商务部统一印制和编号的《中华人民共和国技术出口许可意向书》(以下简称“《技术出口许可意向书》”)。《技术出口许可意向书》的有效期为3年,在《技术出口许可意向书》有效期内,未签订技术出口合同的,则要向地方商务主管部门重新提出出口申请。

在取得《技术出口许可意向书》后,出口企业方可对外进行实质性谈判,并在达成合意后签订技术出口合同。

3.获得《技术出口许可证》:

签订技术出口合同后,持《技术出口许可意向书》、合同副本、技术资料出口清单(文件、资料、图纸、其他)、签约双方法律地位证明文件到地方商务主管部门申请技术出口许可证。地方商务主管部门对技术出口合同的真实性进行审查,并于15个工作日内对技术出口做出是

否许可的决定,对许可出口的技术颁发由商务部统一印制和编号的《中华人民共和国技术出口许可证》。

(四)禁止出口人工智能技术

目前《出口目录》所列禁止出口技术暂不包含人工智能相关技术。但需要注意关注《出口目录》的更新情况。如相关技术被列为《出口目录》中的禁止出口技术,则不得以任何方式出口禁止出口技术。

三、企业人工智能技术出口合规路径

(一)审慎判断技术项目出口行为

人工智能企业在日常经营活动中,应审慎判断经营行为是否可能构成技术出口。在经营中,应当建立了解客户(know your customer,KYC)制度,进行客户信息审查。如客户具有境外因素,则需要注意双方交涉是否构成技术提供,特别是要注意电子邮件沟通等非正式交易活动的内容审查。跨国公司的境内主体在与境外主体进行内部沟通时,需要特别注意沟通内容,避免构成非法技术出口。

(二)正确评估技术出口规制分类

在判定项目属于技术出口行为后,人工智能企业应从技术本质出发,对照《出口目录》按照禁止出口技术——限制出口技术——自由出口技术的顺序进行技术分类定位。如存在定位不确定、定位不清晰情况,应及时与商务主管部门沟通,避免误判。

(三)严格遵守分类出口流程规定

在确定技术分类的定位后,根据不同分类采取不同行动。属于禁止出口技术的,取消出口计划;属于限制出口技术的,严格遵守程序规定进行技术出口许可申请,特别是要注意避免在取得《技术出口许可意向书》之前就对外进行实质性谈判;属于自由出口技术的,积极履行出口合同登记义务。



第二篇 美国人工智能算力管制 对人工智能企业出海的影响及风险规避

一、美国人工智能算力管制政策

(一)美国对人工智能算力硬件管制

根据管制对象的不同,美国出口管制法律法规体系可以分为两部分:军用物项管制和两用物项管制。对于军用物项管制的法律依据主要是《武器出口管制法》和《国际武器贸易条例》,对于两用物项管制的法律依据主要是《2018年出口管制改革法》(Export Controls Reform Act,ECRA)和《出口管理条例》(Export Administration Regulation,EAR)。由于人工智能算力硬件系两用物项,故与之相关的管制法律主要是《2018年出口管制改革法》和《出口管理条例》。

1.《2018年出口管制改革法》

美国2018年颁布的《2018年出口管制改革法》为《出口管理条例》提供了永久性法定授权。同时,该法案扩大了美国出口管制的适用范围,特别是增加了对美国的新兴和基础技术的出口控制,并授权美国总统和美国商务部确定和定义这些技术的构成。2020年10月15日,美国白宫发布《关键和新兴技术国家战略》(“《CET战略》”),《CET战略》中列明了20类关键和新兴技术清单(“2020年CET清单”),后续每两年更新一次关键和新兴技术领域列表,及各领域内的具体技术清单。最新的清单即“2024年CET清单”于2024年2月发布,见下表。

序号	领域名称(英文)	领域名称(中文)	备注
1	Advanced Computing	先进计算	
2	Advanced Engineering Materials	先进工程材料	
3	Advanced Gas Turbine Engine Technologies	先进燃气轮机技术	
4	Advanced and Networked Sensing and Signature Management	先进及网络化传感与特征管理	
5	Advanced Manufacturing	先进制造	
6	Artificial Intelligence	人工智能	
7	Biotechnologies	生物技术	
8	Clean Energy Generation and Storage	清洁能源的生成和储存	

序号	领域名称(英文)	领域名称(中文)	备注
9	Data Privacy, Data Security, and Cybersecurity Technologies	数据隐私、数据安全和网络安全技术	新增
10	Directed Energy	定向能源	
11	Highly Automated, Autonomous, and Uncrewed Systems (UxS), and Robotics	高度自动化、自主化和无人驾驶系统与机器人技术	
12	Human–Machine Interfaces	人机接口	
13	Hypersonics	高超声速	
14	Integrated Communication and Networking Technologies	集成通信和网络技术	
15	Positioning, Navigation, and Timing (PNT) Technologies	定位、导航和授时(PNT)技术	新增
16	Quantum Information and Enabling Technologies	量子信息和使能技术	
17	Semiconductors and Microelectronics	半导体和微电子	
18	Space Technologies and Systems	太空技术和系统	

其中与人工智能产业相关的技术领域包括“先进计算”“人工智能”“数据隐私、数据安全和网络安全技术”“高度自动化、自主化和无人驾驶系统与机器人技术”“半导体和微电子”等。各领域的具体技术清单见下表。

领域名称	具体技术清单
先进计算	先进超级计算,包括AI应用 边缘计算和设备 先进云服务 高性能数据存储和数据中心 先进计算架构 先进建模和模拟 数据处理和分析技术 空间计算
人工智能	机器学习 深度学习 强化学习 感觉感知和识别 AI保证和评估技术 基础模型 生成式AI系统、多模态和大型语言模型 用于训练、调整和测试的合成数据方法 规划、推理和决策 提高AI安全性、信任度、安全性和负责任使用的技术

领域名称	具体技术清单
数据隐私、数据安全和网络安全技术	分布式账本技术 数字资产 数字支付技术 数字身份技术、生物识别和相关基础设施 通信和网络安全 增强隐私的技术 数据融合和提高数据互操作性、隐私和安全性的技术 分布式机密计算 计算供应链安全 增强现实/虚拟现实中的安全和隐私技术
高度自动化、自主化和无人驾驶系统与机器人技术	地面、空中 海上 太空 支持数字基础设施,包括高清(HD)地图 自主指挥和控制
半导体和微电子	设计和电子设计自动化工具 制造工艺技术和制造设备 超越互补金属氧化物半导体(CMOS)技术 异构集成和先进封装 专为人工智能、自然和恶劣辐射环境、射频和光学元件、高功率器件以及其他关键应用而设计的特殊/定制硬件组件 用于先进微电子的新型材料 微机电系统(MEMS)和纳机电系统(NEMS) 非冯·诺依曼计算的新型架构

2.《出口管理条例》

《出口管理条例》是《2018年出口管制改革法》的实施法规,其编入《美国联邦法规》第十五编B分编“商业与外贸有关的法规”的第七章“商务部产业与安全局”下的第C分章。美国国会根据《2018年出口管制改革法案》将其通过控制出口来监管对外贸易的部分宪法权力授权给行政部门,而美国商务部则依据具体实施规则《出口管理条例》行使该权力。

在《出口管理条例》体系内,美国商务部工业与安全局(Bureau of Industry and Security, BIS)针对特定行业领域发布专门规定,作为更为具体的出口管制规则。与人工智能算力相关物项的临时最终规则(Interim Final Rule, IFR)于2022年10月7日首次发布,并于2023年10月17日、2024年4月4日多次调整。经过多次调整,BIS在半导体相关领域的出口管制政策框架已基本搭建完毕,相关重心将逐步向执法和监管方向转移。

3.实体清单制度

实体清单(Entity List, EL)是《出口管理条例》第744部分的附录4(Supplement No. 4 to Part 744—Entity List)。这个清单由美国商务部工业与安全局(BIS)管理,目的是对特定的外国个人和企业实施出口限制。被列入实体清单的最直接影响是在涉及美国产品与技术的出口、转口和转让贸易时必须事先获得美国商务部的许可。清单中的实体按国家排列,并列

出确定实体的名称、已知地址和别名、实体的许可要求范围、其许可政策及其对《联邦公报》的来源引注。截至2024年8月23日,已有845个中国实体被列入清单。

美国众议院在2024年9月10日启动的“中国周”立法行动中启动审议包括《出口管制执法强化法案》(Export Control Enforcement and Enhancement Act,H.R.7151)在内的一系列法案。《出口管制执法强化法案》旨在加快实体清单更新流程,更新清单实体许可政策,大幅强化实体管制力度。

(二)美国对人工智能云算力管制

1.云算力管制起始——人工智能《行政命令》

人工智能云算力,即使用IaaS(Infrastructure as a Service,基础设施即服务)云服务远程获得算力。美国对于IaaS管制起始的法律依据主要为两个总统行政令。

一是特朗普政府2021年13984号令(“E.O. 13984”),授权商务部制定法规,要求美国IaaS提供商验证其外国人客户的身份,以及采取特别措施阻止外国恶意网络行为者使用美国的IaaS产品。

二是拜登政府2023年14110号令(“E.O. 14110”),其核心内容是授权制定规则,拓展身份识别要求的适用范围(将前述身份识别要求拓展至美国IaaS服务上的海外经销商),同时要求IaaS提供商向商务部报告外国用户进行AI大模型训练的交易。

2.云算力管制落实——商务部落实《行政命令》新举措

为落实上述两份总统行政令,推进对IaaS服务的管制,美国商务部工业与安全局(BIS)于2024年1月29日公布了《“采取额外措施应对重大恶意网络活动方面的国家紧急情况”(Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities)拟议规则的通知》(notice of proposed rule making)(以下简称“NPRM”)。根据NPRM,美国IaaS提供商、美国经销商及相关外国经销商须核验外国人客户身份信息,并在特定情形下向美国商务部报告外国人客户的详细身份信息和人工智能大模型训练活动情况。

在人工智能算力硬件出口管制加压的环境下,使用云计算服务获取相关算力资源,原本成为部分人工智能产业链企业的替代方案之一,而NPRM便是针对此替代方案推出的管制对策。

二、美国人工智能算力管制标准

(一)算力硬件出口管制框架基本完成

经过2022年10月7日、2023年10月17日、2024年4月4日多次调整,美国在半导体相关领域的出口管制政策框架已基本搭建完毕,相关重心将逐步向执法和监管方向转移。基本完成的出口管制政策呈现明显的双轨制特征:对于风险系数较低或者管控意义不大的相关物项,放松管控;对于重点监管领域,通过规定更加严格的尽职调查义务强化监管。

1.芯片管制技术标准

2022年10月7日规定ECCN 3A090和4A090类别中的高性能计算设备、芯片以及相应组件,将在满足以下两项条件时受到出口限制:

- (1)芯片的I/O带宽传输速率大于或等于600 Gbyte/s;
- (2)数字处理单元/原始计算单元每次操作的比特长度乘以TOPS计算出的算力之和大于或等于4800TOPS。

2023年10月17日BIS进一步收紧了限制范围:

(1)ECCN 3A090a针对最高性能芯片,集成电路中包含一个或多个处理单元达到以下任一标准:a)综合运算性能(Total Processing Performance,TPP)达到4800,或b)综合运算性能达到1600,同时“性能密度”(Performance Density,PD)达到5.92。

(2)ECCN 3A090b针对次高性能芯片,集成电路中包含一个或多个处理单元达到以下任一标准:a)综合运算性能达到2400但低于4800,性能密度达到1.6但低于5.92;b)综合运算性能达到1600,性能密度达到3.2但低于5.92。

2024年4月4日中规定的新的管制规则主要针对GPU性能进行了细化规定:

4A003类目下“数字计算机”“电子组件”及其相关设备和“组件”,对于所有目的地(除EAR第740部分第1号补充文件国家组E:1或E:2中的国家外),“调整后峰值性能”(“APP”)超过70 Weighted TeraFLOPS(WT,每秒计算万亿次浮点运算,主要针对GPU性能,CPU和NPU主要提供定点/整数算力)的计算机和4A003.c中所述的“电子组件”都需要许可证(NLR)。

2.许可例外适用情形严格排除芯片物项

2023年10月17日新规二次修订时引入适用于先进计算物项的新许可例外“经告知先进计算”(NAC);并在2024年4月4日的新规中进行了细化和拆分,将之分为NAC与“经授权先进计算”(ACA)两个许可例外,以精细化对中国澳门特别行政区和包括中国在内的D:5组国家加强管控。ACA的设立为非重点关注领域(如与数据中心无关的先进计算芯片应用领域)提供相应的贸易便利,简化在原NAC下繁重的通知审查压力。对于重点关注领域,仍将通过NAC的预先告知机制对相关物项的流转严加管控。

在此需要重点提示的是,关于3A090.a项下相关物项(先进计算集成电路和相关的半导体制造设备),其在中国等D:5组国家境内的境内转移不为ACA和NAC等任何一个许可例外所豁免,因此即使目前在中国境内进行相关物项的交易和流转也必须取得BIS的出口许可证。

3.最终用户和最终用途管控强化

2024年4月4日新规加强了在半导体制造供应链上美国出口管制监管要求的传导,以防止相关实体通过第三国获得半导体生产设备的研发和制造能力。这一意图在美国商务部工业与安全局(BIS)于该次新规中发布的相关评议中表现得尤为明显。在第46号评议中,针对评议者所提出的“当向第三方出口用于‘开发’或‘生产’全新外国产物项的物项时,若该等外国产物项今后专用于受限生产设施,即生产‘先进节点集成电路’的设施内,许可证审查义务应在供应链的上游延伸到何种程度?”问题时,BIS表示,相关境外生产者需基于最低成分含量

规则和外国直接产品规则等相关规定在对该外国生产物项分别评估其是否可能属于EAR下受控物项,但是,即使基于相关评估该等外国生产物项不属于EAR下受控物项,若相关境外生产者系通过设计其供应链故意规避相关许可证要求,那么该产品仍需取得许可证,否则将视该等行为为违反EAR相关规定的行为。此外,BIS还进一步表示,在供应链的任何环节,只要知晓相关物项可能会被最终用于受限最终用途,即使涉及一小部分物项,也需就该部分物项取得许可,对于受EAR管控的3B、3C、3D和3E类物品,根据第744.23(a)(2)(ii)节的规定,即使不知晓使用这些物品的“设施”的生产技术节点,也可能需要许可证。

(二)实体清单扩容强化

1.被列入实体清单(EL)对企业经营的影响

所有受EAR管控的物项(包括硬件、软件、技术等)向被列入实体清单的主体出口、再出口或国内转移等,均须向美国商务部申请许可。清单实体无法采购管制硬件,但已经采购的可以使用、加工;无法延期、更新、采购管制软件,但已经获取了License的软件可以在授权期内继续使用;原厂服务无法提供。但实体清单并不禁止客户从清单主体处购买设备或服务。

2.《出口管制执法强化法案》强化实体清单管制

扩大提案权限与简化决策流程是该法案的核心变化。法案赋予最终用户审查委员会(End-User Review Committee)的每个成员直接提议修改实体清单的权力。来自美国国防部、国务院等部门的代表可以根据各自的专业判断,直接提议将特定实体添加到清单中,但最终决定仍需要委员会多数成员的投票通过。同时,委员会必须在30天内对提案进行投票表决,大幅缩短了决策时间。最终用户审查委员会主席可以在特定情况下将投票期延长15天,以获取更多信息。

在许可政策方面,对实体清单上的实体默认采取“推定拒绝”的许可政策,同时允许委员会针对特定实体或特定类型的物项采用不同的许可政策,保留了一定的灵活性。此外,法案还强调了决策过程的民主化,每个委员会成员在相关事项上有一票表决权,包括各部门代表,最终用户审查委员会主席无权单独作出决定或推翻投票结果。

通过赋予美国国防部、国务院等部门更直接的参与权,该法案旨在确保从多角度评估潜在的美国国家安全威胁,并能迅速采取行动。这种机制的变化可能会导致更多实体被列入清单,对全球科技企业,特别是中国企业产生重大影响。

(三)云算力管制铡刀升起

1.云算力身份自由受限

根据NPRM,美国IaaS产品的:i)美国IaaS提供商(包括美国供应商及美国经销商),以及ii)其外国经销商须建立“客户识别计划”(Customer Identification Program, CIP),以执行有效的客户验证机制并维护其外国人客户的身份信息,并且这些CIP需要向美国商务部进行报告。除非商务部部长基于特定对象“阻止滥用IaaS产品”的安全实践能力,而在特定情况下给予了豁免,否则所有潜在“客户”(Customer)及其“受益所有人”(beneficial owner),都会受

制于身份识别。

NPRM 规则要求“美国 IaaS 提供商”及其“美国 IaaS 产品”的“海外经销商”在 IaaS 账户开立前,收集潜在非美国人“客户”或“受益所有人”的以下信息:名称;地址/主要营业地/组建地(含使用 IaaS 产品的地点);付款方式和来源;电子邮件地址;电话联系信息;基于对该等非美国人对账户所有或控制权的核实,收集其用于访问和管理账户的 IP 地址,以及每次访问和管理的日期和时间。

2.云算力训练报告制度

NPRM 要求“美国 IaaS 提供商”及其“美国 IaaS 产品”的“海外经销商”对与其交易的外国人进行训练“具有可能用于恶意网络活动的潜在能力的大型 AI 模型”的行为,向商务部部长提交报告。所谓“具有可能用于恶意网络活动的潜在能力的大型 AI 模型”在 NPRM 中被定义为“任何具有‘两用基础模型’技术条件或具有其他相应技术参数,并且可用于协助或自动化开展恶意网络活动的人工智能模型,包括但不限于社会工程学攻击、漏洞发现、拒绝服务攻击、数据中毒、目标选择和优先排序、虚假信息或错误信息的生成和/或传播,以及远程指挥和控制。”

上述报告内容除 CIP 内容外,还需含有“训练运行的信息”,包括:训练中计算运行的估计次数;训练运行预计开始和结束的日期;训练运行加速器中使用的主要 AI 模型;确保对经训练的模型权重进行安全存储和保护访问的政策和流程;过去四年中发生的任何导致未经授权访问模型权重或源代码,或其他重大损害的网络安全或内部威胁事件。

NPRM 授权美国商务部对“大量外国人员提供美国 IaaS 产品用于恶意网络活动,或有大量外国人员直接获取美国 IaaS 产品用于恶意网络活动”的情形可以自行启动调查,评估相关证据,并且决定是否实施特别措施。如果商务部部长确定有证据表明应实施特别措施,将在《联邦纪事》上发布决定。可能采取的特别措施包括:(1)针对某些外国司法管辖区内的客户、潜在客户或账户持有者实施于美国 IaaS 提供商处开设或维持账户(包括经销商账户)的限制或附加条件;(2)针对某些特定的外国人实施在美国 IaaS 提供商处开设或维持账户(包括经销商账户)的限制或附加条件。

三、人工智能企业应对美国算力出口管制的合规建议

(一)股权代持是否符合监管规范?

股权代持,也称为代持股或隐名持股,是一种商业实践,其中一方(名义股东)在法律上持有股份,而实际的利益所有者(实际股东)则不公开地享有股份带来的利益。使用股权代持制度应对美国出口管制,可能会引发下列问题。

1.实体控制问题

美国出口管制法规不仅关注直接出口行为,还关注对实体的控制。如果实际股东或最终受益所有人(beneficial owner)是受《出口管理条例》约束的个人或实体(例如,受制裁的个人或位于受制裁国家/地区的实体),那么即使名义股东是合规的,股权代持安排也可能违反《出

口管理条例》。

2.透明度要求

《出口管理条例》要求在涉及受管制物品的出口、再出口或转让(国内)时,必须披露所有相关的信息和利益方。股权代持可能阻碍这种透明度,从而违反法规。

3.许可要求

如果股权代持的目的是规避对特定个人或实体的出口限制,那么这种安排可能会被视为违反《出口管理条例》。例如,如果某个实体或个人被禁止接收特定技术或产品,而通过股权代持来间接获取这些技术或产品,那么这种行为可能被视为违规。

4.否认条款

《出口管理条例》包含否认条款,禁止任何旨在规避法规的交易或行为。即使股权代持在技术上不违反任何具体规定,但如果其目的是规避出口管制,则可能被视为违反否认条款。

(二)信托模式能否实现资产保障?

信托模式可以在一定程度上用于资产管理和保障,但在应对美国出口管制时,其效果取决于多种因素,必须谨慎设计和操作,以确保符合相关法规。

1.信托结构与控制权

信托可以用于隔离资产,减少个人或实体对资产直接控制的风险。然而,如果信托的受益人、设立人或其他相关方受到美国出口管制的限制,信托资产可能仍然受到管制。

2.受益人的影响

如果信托的受益人是受制裁的个人或实体,或者位于受制裁的国家或地区,那么即使资产被置于信托中,也可能受到美国出口管制的限制。

3.资产性质

信托中的资产如果是受EAR管制的物品(如特定技术、软件或设备),那么即使这些资产被置于信托中,其出口、再出口或转让(国内)也可能需要遵守EAR的规定。

4.受托人的责任

受托人有责任确保信托的操作符合所有适用法律,包括出口管制法规。如果受托人未能履行这一责任,可能会导致信托资产受到处罚或限制。



第三篇 美国大模型管制对我国人工智能出海影响剖析与应对措施

一、美国大模型管制政策概述

(一)美国大模型管制政策的背景

2024年5月8日,美国众议院外交事务委员会(Committee on Foreign Affairs)提出《增强关键出口海外限制国家框架法案》(H.R.8315–Enhancing National Frameworks for Overseas Restriction of Critical Exports Act,即《ENFORCE法案》)。该法案核心内容是对《2018年出口管制改革法》(Export Control Reform Act of 2018,ECRA)的修订,将使美国政府更容易对人工智能模型实施出口管制,以保护美国人工智能及其他支持技术免受外国对手的利用。

《ENFORCE法案》涵盖了包括人工智能系统以及对国家安全至关重要的特定新兴和基础技术,特别将为美国出口、再出口或在美国国内转移某些物项建立许可要求。此外,在设计、开发、生产、使用和操作方面,也将受许可要求的约束。5月22日,美国众议院外交事务委员会进行了对这项新法案的首轮投票,结果显示有43票赞成,3票反对。美国众议院计划在9月第3周对一系列与中国相关的法案进行投票(“中国周”),其中就包括了《ENFORCE法案》。

(二)法案对大模型相关概念的定义

1.人工智能及人工智能系统的定义

《ENFORCE法案》在第二节中对人工智能及人工智能系统给出了定义。其中,其对于人工智能系统的定义,参照了2020年《国家人工智能倡议法案》(H.R.6216–15 U.S.C. 9401(3))第5002(3)条之规定,即“‘人工智能’这个术语指的是一种基于机器的系统,该系统能够针对一组由人类定义的目标,对真实或虚拟环境做出预测、推荐或影响决策。人工智能系统利用机器和基于人类的输入:(A)感知真实和虚拟环境;(B)通过自动化分析,将这种感知抽象成模型;(C)使用模型推理来制定信息或行动的选项。”

对于人工智能系统,法案中将其定义为:“‘人工智能系统’指的是任何人工智能的软件或硬件实现,包括人工智能模型权重和与人工智能实现相关的任何数值参数。”

2.受监管人工智能系统的临时定义与最终定义

《ENFORCE法案》第2节对受本法案监管的人工智能系统采取了双重定义方式,首先通过“临时定义”确定一个初步的规制范围,帮助立法者和利益相关者理解本法案的意图,并为后续修订提供了基础,使得在讨论过程中可以更容易地修改和澄清术语;“最终定义”则需要

通过充分讨论并结合实践在一定期限内确定,作为后续法律解释和执行的基础,为法律实施提供明确的指导。

(1) 受监管人工智能系统的临时定义及构成分析

受监管人工智能系统的临时定义的有效期为法案生效之日起至最终定义发布之日止。“‘受监管的人工智能系统’指的是一个符合以下条件的人工智能系统:(I) 展示或可预见被修改后表现出能够在对美国国家安全和/或外交政策构成严重风险的任务中体现高水平性能的能力,即使它向最终用户提供了试图阻止用户利用相关能力的技术保障,例如(aa)大幅降低专家或非专家设计、合成、获取或使用化学、生物、放射性或核(CBRN)武器或大规模杀伤性武器的门槛;(bb)通过自动匹配的漏洞发现和利用,针对广泛的潜在网络攻击目标,实现攻击性网络行动;或(cc)允许通过欺骗或混淆手段逃避人为控制或监督;或(II)可以合理预期它将表现出第(I)分款所述的能力,例如展现或者意外地展现相关能力模型的技术相似或具有同等表现。”

总体而言,《ENFORCE 法案》拟监管的人工智能系统能够对美国国家安全和/或外交政策构成严重风险,能表现出高水平性能的能力,或者本不具备该能力但在经过修改后可具备该能力。同时,该定义的标准在于人工智能系统是否客观地具备上述能力,即便系统能够提供技术保障以防止用户利用该能力,也不能得到监管上的豁免。

对于上述受监管人工智能系统的临时定义,法案通过“举例+兜底”的方式进行具体确定。提供的例示包括:大幅降低设计、合成、获取或使用化学、生物、放射性或核(CBRN)武器或大规模杀伤性武器的门槛;通过自动匹配的漏洞发现和利用,针对广泛的潜在网络攻击目标,实现攻击性网络行动;允许通过欺骗或混淆手段逃避人为控制或监督。同时,通过兜底条款保证了监管范围的可解释性,避免监管漏洞的发生:人工智能系统如果被合理预期具有上述能力,即可被认定为受监管人工智能系统,例如具有上述受监管人工智能系统所具有的技术上的相似性或等效的性能。

(2) 受监管人工智能系统的最终定义

上述临时定义将在后续工作中进行更新,并被确定为最终定义。受监管人工智能系统的最终定义由商务部长会同国务卿、国防部长、能源部长在法案颁布后365天内协商决定。协商中需综合考虑技术和非技术因素,特别是最能有效提升美国国家安全的因素。

(三) 美国大模型管制的涵盖范围

1. 对人工智能模型不做是否开源的区分

从上述“受监管人工智能系统”的定义来看,《ENFORCE 法案》拟监管的人工智能系统未区分是开源系统还是闭源系统。理论上,无论人工智能系统是开源还是闭源,均有被认定为“受监管人工智能系统”的可能,取决于是否能够对美国国家安全和/或外交政策构成严重风险,是否能表现出高水平性能的能力。

2. 明确对人工智能模型权重的监管

根据《ENFORCE 法案》中对于“人工智能系统”的定义,“人工智能模型权重”如果(可能)对美国国家安全和/或外交政策构成严重风险,被明确列入监管范围。

“人工智能模型权重”是指人工智能模型中每个神经元连接的参数。这些权重在训练过程中不断调整,以使模型能够更准确地预测输出。简单来说,模型权重决定了输入数据如何通过模型被处理和转换。人工智能模型权重在模型中的作用类似于人类大脑中的神经连接强度。不同权重组合让模型能够识别和分类各种复杂的模式。模型权重是模型智能的核心部分。由于诸多人工智能模型在训练初期,需要参考成熟的人工智能模型权重来进行部署和优化,以提升模型能力和准确度,因此,对于人工智能模型权重的监管,将直接影响相关模型的搭建与训练。

3.对“与人工智能实现相关的任何数据参数”加以监管

除人工智能模型权重外,《ENFORCE 法案》中对于“人工智能系统”的定义还包括“与人工智能实现相关的任何数据参数”。这些数据参数,如果对美国国家安全和/或外交政策构成严重风险,亦被明确列入监管范围。“人工智能实现”(Artificial Intelligence Implementation)指将人工智能技术应用到实际问题 and 场景中的过程。与之相关的数据参数包括数据质量参数、数据特征参数、数据预处理参数、模型训练参数、模型评估参数、超参数等,上述人工智能模型权重即属于“模型训练参数”。“与人工智能实现相关的任何数据参数”是人工智能模型搭建、优化、应用等过程中均不可缺少的内容,是人工智能技术的核心。可以认为,该“人工智能系统”的定义涵盖了与人工智能模型相关的几乎全部关键信息,对数据参数的监管,可有效实现立法者的监管目的。

(四)《ENFORCE 法案》对《2018 出口管制改革法》的修正

1.明确总统对人工智能系统的监管权力

《ENFORCE 法案》通过对《2018 出口管制改革法》的修正,赋权总统控制涉及特定人工智能系统和新兴技术的美国人的活动,无论他们身处何处,因为这些技术被认定为对美国国家安全至关重要。由于《2018 出口管制改革法》无失效时间,通过本修正,即可以实现总统对人工智能系统监管的永久授权。

2.增设商务部对人工智能系统监管的额外权力

《ENFORCE 法案》明确了人工智能系统的监管部门、监管范围。监管部门为总统授权商务部实施许可证管理。监管范围包括物品交易许可与服务提供许可等。即美国人在出口、再出口或者国内转移被确定为对美国国家安全至关重要的新兴和基础技术,或者可能支持设计、开发、生产、使用、操作、安装、维护、修理、检修或者翻新这些系统的技术或相关服务时,美国总统有权要求上述相关人员申请并获得商务部许可。

二、我国人工智能出海受美国大模型管制的可能影响

(一)美国大模型管制对我国人工智能出海影响重大的原因

1.我国人工智能模型依赖美国大模型开源框架

我国企业在其人工智能应用的开发过程中,普遍倾向于采用国际上成熟且功能强大的开

源框架,其中,TensorFlow和PyTorch这两种由美国企业开发的框架尤为受到青睐。TensorFlow由谷歌推出,以其灵活性和易于扩展的特点在业界享有盛誉;而PyTorch则由Facebook(现Meta)研发,以其直观的编程模型和动态计算图功能在研究社区中广受欢迎。由此,我国人工智能模型不可避免地将会受到这些开源框架在核心算法、模型架构、技术更新、社区支持等方面的限制与制约。

2.我国人工智能模型惯用美国预训练模型

在自然语言处理(NLP)领域,预训练模型因其强大的语言理解和生成能力而成为行业的重要基石。其中,由美国公司OpenAI开发的GPT模型,以其庞大的参数规模和卓越的性能,在全球范围内受到了广泛的关注和应用。中国的人工智能企业也不例外。企业通过购买OpenAI的API服务来接入GPT模型。这种方式允许企业无需自行训练和维护庞大的模型,即可快速实现产品中的自然语言处理功能。企业可以通过发送请求到OpenAI的API,接收模型生成的文本或执行特定的NLP任务,如文本摘要、问答系统、语言翻译等。同时,为了更好地适应特定的业务场景和用户需求,企业可以在GPT等预训练模型的基础上进行微调。微调通常涉及使用企业自己的数据集对模型进行进一步的训练,以优化模型的性能和适应性。通过这种方式,企业能够将GPT模型集成到自己的产品中,提供更加定制化的语言处理服务。

(二)我国人工智能出海可能遭遇切实影响

1.交易活动受限

《ENFORCE法案》强化了美国商务部对人工智能相关的物项取得与交易活动的许可管理。我国人工智能企业在涉及美国要素的交易活动中,将不得不遵循更为复杂的许可申请流程。这包括但不限于提交详细的产品描述、技术规格、预期用途、交易双方信息等,以确保符合美国商务部的审查标准。除增加交易成本外,许可申请可能会带来不必要的延迟,影响合同履行、项目进度和市场机遇等诸多方面。

2.技术发展受限

如《ENFORCE法案》对美国大模型开源框架和预训练模型实行出口监管,会影响使用上述美国大模型技术的我国人工智能企业带来合规压力。企业一方面需要投入更高成本调整框架、重构模型,另一方面可能导致现有产品或服务交付停滞而产生违约责任。同时,我国人工智能企业可能面临无法获得及时技术更新,遭遇技术封锁等问题。

3.国际合作受阻

《ENFORCE法案》加强监管力度,可能使得国际合作伙伴对我国人工智能企业的技术和服

务产生信任危机。他们可能会更加谨慎地评估与我国企业的合作风险,担心触犯美国的出口管制规定。这种审慎的态度可能会导致合作进程的延缓,甚至有可能导致正在进行的合作项目中断,从而对我国企业的国际业务拓展造成不利影响。同时,频繁的监管问题可能会损害我国企业的国际品牌形象,影响其在全球市场的竞争力。

4.合规成本加剧

《ENFORCE法案》的出台意味着中国企业在出海过程中需要更加关注美国市场的法律法规,特别是与人工智能相关的法规以及相关规定,与此同时,需要关注相关法律法规中提及

的义务要求,如《ENFORCE 法案》中的许可证要求,可能会间接导致我国企业合规成本增加,增添运营复杂性。

三、我国人工智能企业的应对措施

(一)梳理企业内部美国大模型使用情况

企业应当立即启动内部审查程序,全面梳理和排查现有技术栈中涉及美国大模型的使用情况。这包括但不限于识别依赖的美国技术、评估潜在的法律风险,以及预测可能的业务中断影响。通过这一过程,企业可以清晰地了解自身对美国技术的依赖程度,为制定应对策略提供依据。同时,企业应当建立详细的记录和跟踪系统,确保在未来的技术研发和业务拓展中,能够有效管理和控制相关风险。

(二)使用欧盟或其他地区大模型作为替代

为了降低对美国大模型的依赖,企业可以考虑转向欧盟或其他地区的大模型作为技术替代。这要求企业进行充分的市场调研和技术评估,以确保所选模型能够满足产品和服务的要求。同时,企业需要与替代模型的供应商建立稳定的合作关系,确保技术支持和服务的连续性。此外,企业还应关注替代技术的合规性和知识产权问题,避免新的法律风险。

(三)发展与培育国内自研大模型基础架构

长期而言,我国人工智能企业应当致力于发展和培育具有自主知识产权的大模型基础架构。这需要企业加大研发投入,吸引和培养顶尖人才,推动技术创新。同时,企业应当与国内高校、科研机构等建立合作关系,共享资源,共同推动国内AI大模型技术的发展。通过自研大模型,企业不仅可以减少对外部技术的依赖,还能在市场竞争中占据有利地位。

(四)统一大市场背景下打造人工智能全产业链

在“建设全国统一大市场”的政策背景下,我国人工智能企业应当抓住机遇,整合资源,打造涵盖数据采集、处理、模型训练、应用开发等环节的全产业链。这不仅有助于优化资源配置,提高产业效率,还能增强企业间的协同效应,共同应对外部挑战。企业应当积极参与行业标准制定,推动产业链上下游的深度融合,共同打造具有国际竞争力的人工智能生态系统。

(五)严判人工智能出海是否违反相关管制政策

在国际化进程中,我国人工智能企业必须高度重视合规问题,严格判断人工智能产品的出海活动是否违反相关国家和地区的管制政策。企业应当建立专业的合规团队,密切关注国际政治经济形势,及时调整出海策略。同时,企业需要建立健全的风险评估和预警机制,确保在复杂多变的国际环境中,能够有效规避法律风险,保障企业的合法权益。



宁人律师事务所
NING REN LAW FIRM

