

new

中倫律師事務所
ZHONG LUN LAW FIRM

& DIGITAL TRANSFORMATION

infrastructure

—
新基建与
数字化转型：
机遇与挑战





中伦研究院出品



CONTENTS /



前言 007

/ 第壹章

导引篇 008

01/ 新基建的政策红利

02/ 新基建之内涵

03/ 企业数字化转型:To be or not to be?

04/ 拥抱数字化转型的新机遇、应对法律挑战

/ 第贰章

应用篇 016

01/ 新基建投资背景下PPP-ICT项目交易结构设计要点 018

02/ 中国自动驾驶行业的主要法律规制及实务 026

03/ 高精地图产业法律问题 033

04/ 数字金融的应用、监管及合规思考 059

— CONTENTS





/ 第三章

开发与知识产权保护篇	068
01/ 人工智能生成物能否获得法律保护?	070
02/ 科技企业的上市中知识产权风险的防范	081
03/ 企业进行人工智能技术开发和技术保护路径探析	104

/ 第四章

合规运营篇	116
01/ 科技企业上市的数据合规	118
02/ 人工智能之间达成“垄断协议”? 算法合谋的反垄断法律风险分析	136
03/ “大数据从何而来”,涉足大数据业务需留意的 “网络爬虫”技术的合规风险	144
04/ 外商投资“新基建”需要注意哪些监管问题	152
05/ 智能家居出海的八个数据保护关键词	159
06/ 移动互联网产品跨境的合规风险与对策	169



PREFACE



2020年初以来,为应对新冠肺炎疫情给我国经济带来的巨大冲击,党中央国务院围绕新型基础设施建设(以下简称“新基建”)进行了一系列重要决策部署,市场随之积极跟进,新基建迎来投资建设的热潮。5月22日,新基建首次出现在政府工作报告中:“加强新型基础设施建设,发展新一代信息网络,拓展5G应用,建设充电桩,推广新能源汽车,激发新消费需求、助力产业升级。”把握好疫情为数字化转型带来的机遇,搭上数字化转型的时代列车,就是抓住了企业在危机中生存与逆势发展的关键。

数字化转型意味着企业将不断开发应用新技术,拓展新领域,构建新的商业模式,而数字化项目的运营路径、知识产权保护、资本注入,以及数据安全与保护都要与飞速发展的新技术相适应,整个行业生态也将迎来一场全面的“重塑”。全面而准确地把握新的法律视角,积极统筹应对新的法律风险,方能使企业在新基建的浪潮中挖掘创造新的核心竞争力,更上一层楼。

中伦律师在传统基础设施建设与“互联网+”时代不断学习,锐意进取,积累了丰富的法律实务经验。面对新基建带来的新一轮机遇与挑战,中伦竭诚希望与企业客户共同成长,为我国经济高质量发展贡献一份力量!

中伦研究院

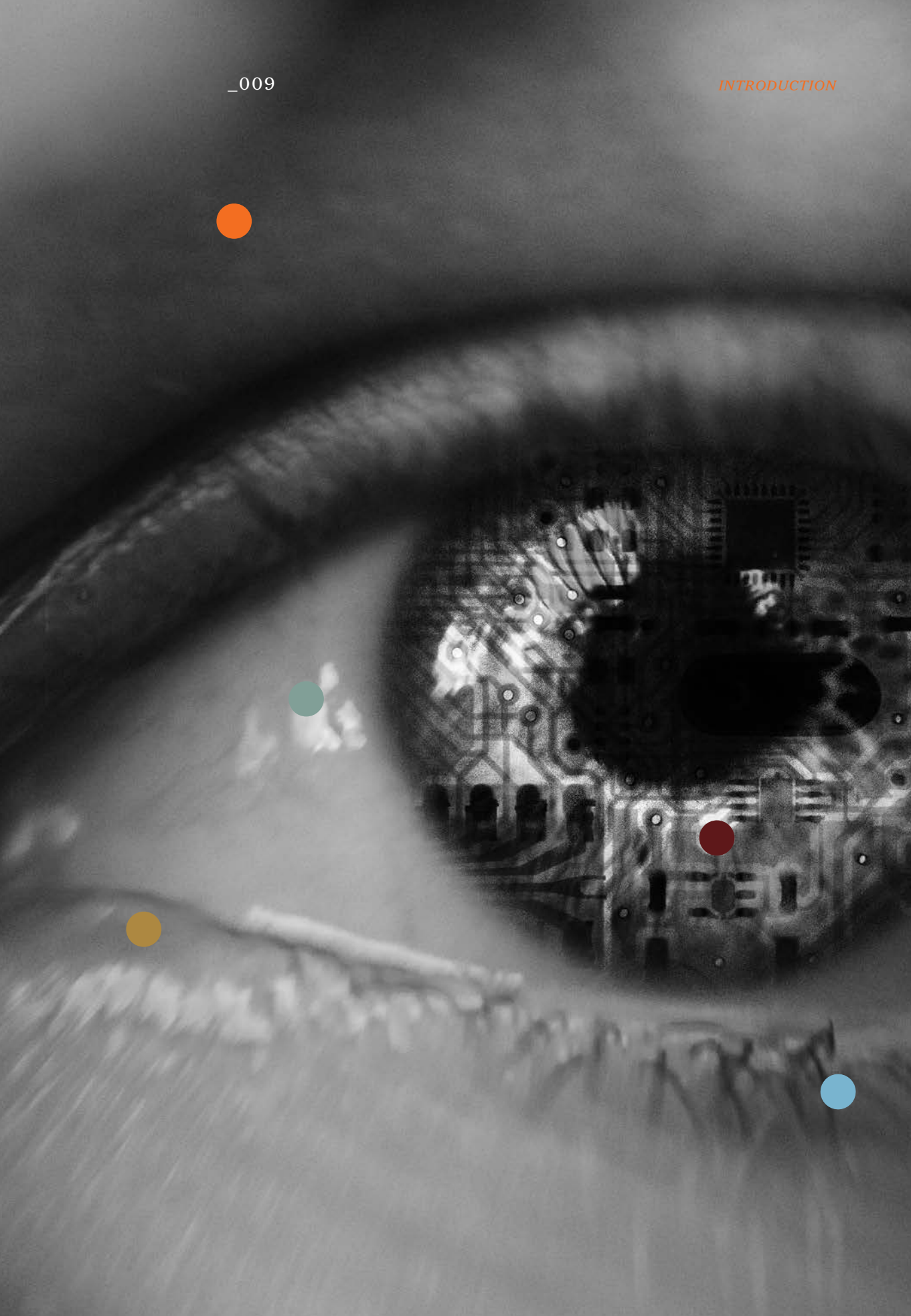
CHAPTER
ONE

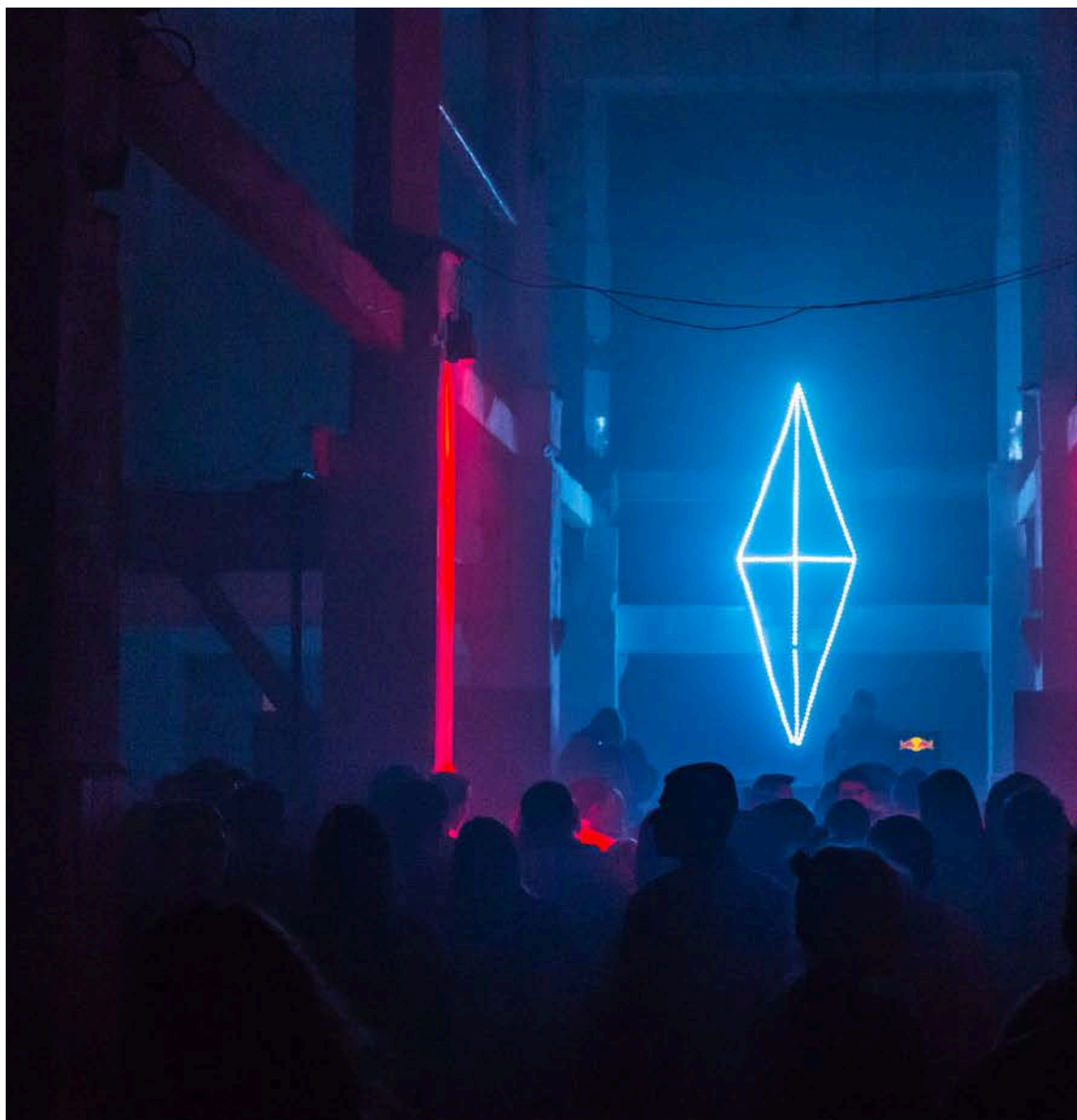
INTRODUCTION



导引篇

CHAPTER ONE





新基建与数字化转型： 疫后经济复苏的新引擎

1.《“新基建”政策白皮书》，赛迪智库 <http://ccid-wisec.com/plus/view.php?aid=16389&tyid=3>

2.《逆周期调节政策加码 二季度经济增速料反弹》，中国证券报 http://www.xinhuanet.com/finance/2020-03-29/c_1125782904.htm

SECTION 001

新基建的政策红利

2020年初，新冠病毒席卷全球，各国面临经济下行的巨大压力。2020年3月，中央政治局常务委员会召开会议提出，加快5G网络、数据中心等新型基础设施建设（“新基建”）进度。

2020年4月1日，习近平总书记在浙江考察时强调：“要抓住产业数字化、数字产业化赋予的机遇，加快5G网络、数据中心等新型基础设施建设，抓紧布局数字经济、生命健康、新材料等战略性新兴产业、未来产业，大力推进科技创新，着力壮大新增长点、形成发展新动能。”

在中央密集政策部署之下，市场开始热烈跟进，新基建迎来风口。截至4月中旬，已有13个省区市发布了2020年新基建相关重点项目投资计划，其中8个省份公布了计划总投资额共计33.83万亿元。

与传统“铁公基”相对应的“新基建”，是服务于国家长远发展和“两个强国”建设的战略举措¹，新基建作为逆周期主要（经济）调节政策之一，其外部效应明显优于传统基建的范畴，发力方向与我国经济长期转型方向相匹配²。其概念发展和促进政策的脉络如下：

时间	会议	内容
2018年12月	中央经济工作会议	加快5G商用步伐，加强人工智能、工业互联网、物联网等新型基础设施建设，加大城际交通、物流、市政基础设施等投资力度，补齐农村基础设施和公共服务设施建设短板。
2019年3月	全国两会政府工作报告	加大城际交通、物流、市政、灾害防治、民用和通用航空等基础设施投资力度，加强新一代信息基础设施建设。
2019年7月	中共中央政治局会议	要稳定制造业投资、实施补短板工程、加快推进信息网络等新型基础设施的建设。
2019年12月	中央经济工作会议	要着眼国家长远发展，加强战略性、网络型基础设施建设，推进川藏铁路等重大项目建设，稳步推进通信网络建设，加快自然灾害防治重大工程实施，加强市政管网、城市停车、冷链物流等建设，加快农村公路、信息、水利等设施建设。
2020年1月3日	国务院常务会议	大力发展先进制造业，出台信息网络等新型基础设施投资支持政策，推进智能、绿色制造。
2020年2月14日	中央全面深化改革委员会第十二次会议	统筹存量和增量、传统和新型基础设施发展，打造集约高效、经济适用、智能绿色、安全可靠的现代化基础设施体系。

时间	会议	内容
2020年2月21日	中央政治局会议	加大试剂、药品、疫苗研发支持力度,推动生物医药、医疗设备、5G网络、工业互联网等加快发展。
2020年2月23日	中央统筹推进新冠肺炎疫情防控和经济社会发展工作部署会议	智能制造、无人配送、在线消费、医疗健康等新兴产业展现出强大成长潜力。要以此为契机,改造提升传统产业,培育壮大新兴产业。
2020年3月4日	中央政治局常务委员会会议	加快5G网络、数据中心等新型基础设施建设进度。
2020年3月6日	工信部加快5G发展专题会	加快5G网络建设步伐。丰富5G技术应用场景,培育新的经济增长点。壮大产业生态,持续提升5G安全保障水平。
2020年4月20日	国家发展改革委4月份新闻发布会	首次明确新基建的范围,主要包括信息基础设施、融合基础设施、创新基础设施三个方面内容,提出重点做好四方面工作。并首次将卫星互联网纳入新基建的范畴。

SECTION 002

新基建之内涵

2020年4月20日,国家发改委在新闻发布会上首次明确了新型基础设施的范围。新型基础设施是以新发展理念为引领,以技术创新为驱动,以信息网络为基础,面向高质量发展需要,提供数字转型、智能升级、融合创新等服务的基础设施体系。主要包括以下三方面内容:

一是信息基础设施。包括以5G、物联网、工业互联网、卫星互联网为代表的通信网络基础设施,以人工智能、云计算、区块链等为代表的新技术基础设施,以数据中心、智能计算中心为代表的算力基础设施等。

二是融合基础设施。主要指深度应用互联网、大数据、人工智能等技术,支撑传统基础设施转型升级,进而形成的融合基础设施,比如,智能交通基础设施、智慧能源基础设施等。

三是创新基础设施。主要是指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施,比如,重大科技基础设施、科教基础设施、产业技术创新基础设施等。

因此,新基建就是数字化的基础设施建设,为中国数字经济的发展和企业的数字化转型搭建高速路、大舞台。相比传统基建,科技创新驱动、数字化、信息网络这三个要素是所有关于新基建认知中的最大公约数,也是中国下一步经济发展的主要路径。



与我们所熟悉的传统项目的建设和运营不同, 数字化项目的市场准入、运营方式、开发模式等都与传统项目有较大的区别。

SECTION 003

企业数字化转型: To be or not to Be?

突发疫情黑天鹅之下,没有企业可以幸免,全球经济将迎来衰退将是大概率事件。

我们观察,疫情冲击下企业命运也各不相同。从统计数据来看,在2020年一季度市场整体消费同比下降19.0%的情形下,线上消费平稳增长,一些大型电商平台3月份网络零售额同比增长10%左右,5G远程医疗、云计算、大数据、人工智能、在线教育、在线医疗、远程办公、生鲜电商、数字营销、高精地图等数字业务形态逆势成长。在全球贸易“碎片化”和“逆全球化”的趋势下,运用跨境电商工具也必将成为中国企业的生存技能。

促进企业数字化转型也是中央会议的热点议题——“加大新投资项目开工力度,加快在建项目建设进度。加大试剂、药品、疫苗研发支持力度,推动生物医药、医疗设备、5G网络、工业互联网等加快发展”³;“推出增设跨境电子商务综合试验区、支持加工贸易、广交会网上举办等系列举措,积极应对疫情影响努力稳住外贸外资基本盘”⁴;“部署加快推进信息网络等新型基础设施建设,推动产业和消费升级,以‘一业带百业’,既助力产业升级、培育新动能,又带动创业就业,利当前惠长远”⁵。这些无疑是企业数字化转型的政策利好信息。

企业数字化转型已经不是一个可选项,而是一个“to be or not to be”的问题,把握好疫情为数字化转型带来的契机,搭上数字化转型的时代列车,就是抓住了企业生存与发展的关键。

SECTION 004

拥抱数字化转型的新机遇、应对法律挑战

“数字化转型(Digital Transformation)是以新建一种商业模式为目标的高层次转型,”⁶进而使公司在一个新的数字化商业环境中发展出新的业务和新的核心竞争力。

当然,数字化转型中,企业会面临一系列的挑战。在法律领域,我们可以预见的法律挑战包括:

- 数字化项目的合法运营路径。与我们所熟悉的传统项目的建设和运营不同,数字化项目的市场准入、运营方式、开发模式等都与传统项目有较大的区别。以自动驾驶项目为例,项目建设和运营会产生一系列诸如

3. 2020年2月21日中共中央政治局会议。
<http://www.12371.cn/2020/02/21/AR-T11582291740139117.shtml>

4. 2020年4月7日国务院常务会议。
http://www.gov.cn/premier/2020-04/07/content_5499975.htm

5. 2020年4月28日国务院常务会议。
http://www.gov.cn/premier/2020-04/28/content_5507096.htm

6. 陈劲, 杨文池, 于飞. 数字化转型中的生态协同创新战略——基于华为企业业务集团(EBG)中国区的战略研讨. 清华管理评论, 2019, P.22-26

增值电信许可和测绘资质要求等。这些项目的合法建设和运营需要新的法律视角和法律导引。

- 数字化技术的知识产权保护。数字化技术的开发需要长期的资金和人力投入,从而形成企业“看不见”的核心竞争力。如果这些技术成果得不到妥善的法律保护,会导致企业竞争力的丧失,进而使得企业的长期投资打了水漂。与此同时,如果企业不能相同地规划知识产权保护政策,进行必要的侵权风险防范,企业还会面临侵权的陷阱。

- 新基建和数字化项目与资本市场的结合。新基建项目需要密集的资金投入,企业在数字化转型中也会面临资金与财务问题。学会与资本市场的结合,合法合规的引入外商投资,可以使得企业“以小博大”,加速企业的发展,与社会分享数字化发展的红利。

- 网络安全与数据保护。在我们所处的5ABCD(5G, AI, Block Chain, Cloud, big Data)时代,“没有网络安全,就没有国家安全”,数据是企业的核心资源和竞争力。企业数字化转型过程中,网络安全法定义务的落实,数据保护体系的建设,关乎企业的合规运营,也关乎企业的命运,即“合规则生,不合规则亡”。

- 数字经济的竞争、滥用和伦理等问题。诸如人工智能和大数据等数字技术可以被应用于很多有益的场景,也会被用于“作恶”,技术是中性的,但是技术的应用是一把双刃剑。因此,数字技术会产生诸如“大数据歧视”、“人工智能滥用”等一系列问题。对新技术的规制是保证“技术向善”的前提。

可以说,数字化新基建对于企业来说,既是对既往业务领域的升级改造,也是对全新业务领域的探索,对整个行业生态来说,我们认为这将是一场全面“重塑”。

面对疫情带来的冲击,如何助力企业乘着新基建的东风转危为机,是许多企业当前面临的首要问题。在这份法律文集当中,我们将从行业应用、开发与知识产权保护,以及合规运营三个方面,针对企业在新基建相关的创新技术开发与应用、投融资过程中可能涉及的法律问题进行梳理与分析,结合中伦在相关领域丰富的法律经验,与企业客户共同迎接新一轮的机遇,为国家新型基础设施建设贡献一份力量。

CHAPTER
TWO

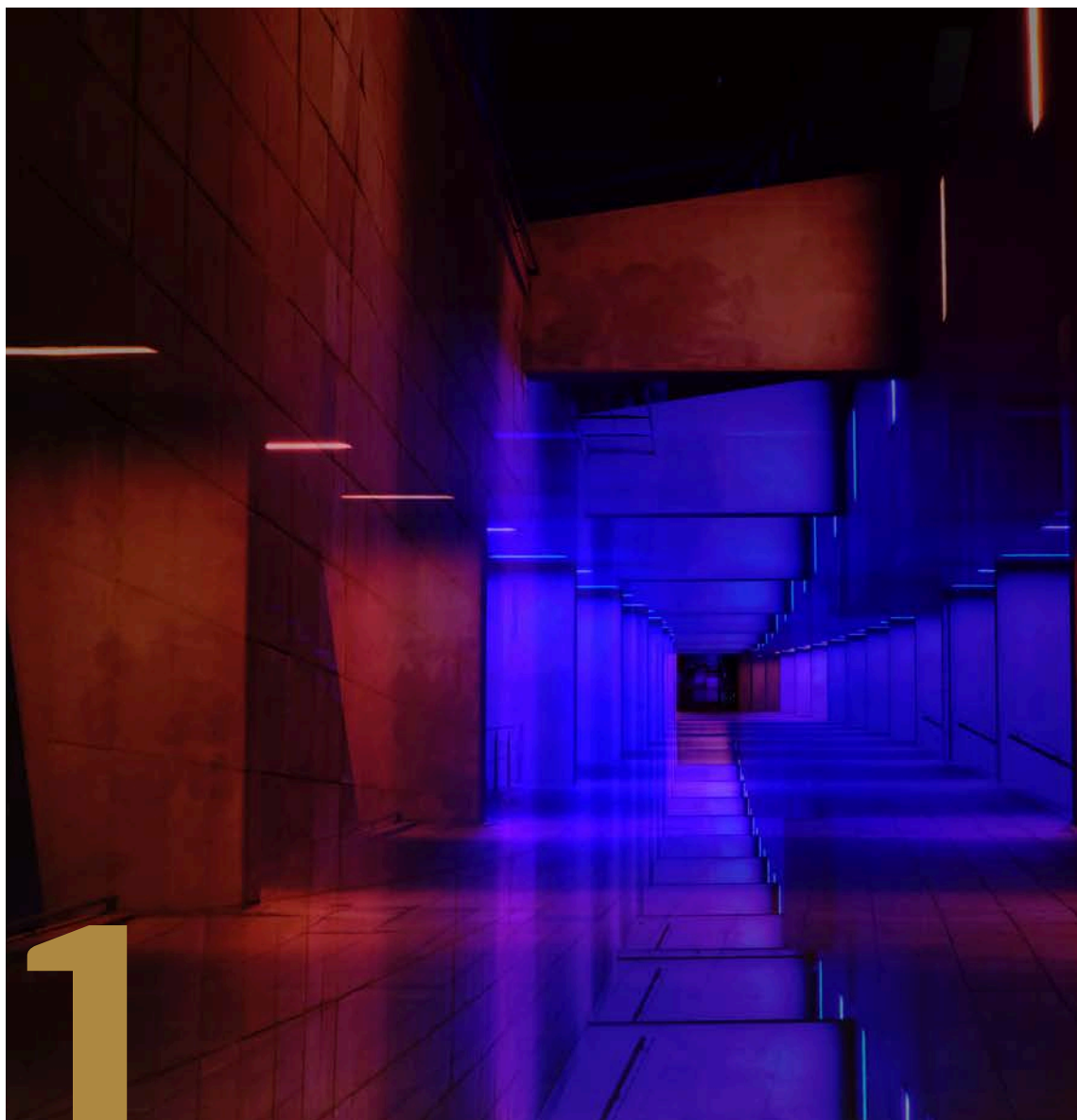
APPLICATION

貳

应用篇

CHAPTER TWO





1

CHAPTER 02

“新基建”投资背景下PPP-ICT项目 交易结构设计要点

作者:周月萍/周兰萍

在当前经济下行和疫情影响下,基础设施建设在稳投资中的作用与重要性再次凸显出来,与此同时,“新基建”一词也成了近期市场热议的话题。作为“新基建”的重要组成部分,国家将会鼓励加大在信息与通信技术(ICT)领域内的投资力度,来解决基础设施补短板的客观需求,实现我国产业的转型升级,释放更多的经济潜力。同时,ICT项目的落地也离不开社会资本的广泛参与,未来将会有更多以政府和社会资本合作(PPP)模式实施的ICT项目受到市场关注。

SECTION 001

“新基建”背景下的ICT与PPP

2020年3月4日，中共中央政治局常务委员会召开会议提出加快5G网络、数据中心等新型基础设施建设进度。据报道，近期全国多个省市发布了2020年重大投资项目，累计公布的计划投资额高达逾数十万亿。

本质上，“新基建”主要是指与数字经济相关的新型基础设施，而根据我国《国民经济行业分类》，制造信息处理与传输载体的产业和通过电子手段满足信息处理和通信的服务业统称为ICT (information and communications technology) 产业，因此对于“新基建”的高度关注必然将带动未来ICT产业的蓬勃发展。与此同时，此次疫情也暴露出各地政府在信息化建设和城市管理上的薄弱以及城乡区域发展间的差距，如何有效解决新型基础设施的短板问题，实现城市信息化管理的功能提升也将会是各地政府面临的一大课题。

政府和社会资本合作 (Public-Private Partnership, PPP) 模式则是自2014年开始中央及各部委鼓励采用的新型基础设施和公共服务投融资模式，主要指地方政府采取竞争性方式择优选择具有投资、运营管理能力社会资本，双方按照平等协商原则订立合同，明确责权利关系，由社会资本提供公共服务，政府依据公共服务绩效评价结果向社会资本支付相应对价，保证社会资本获得合理收益。近年来，PPP模式已在基础设施(如公路、铁路、隧道等)和社会公共服务(如医疗、文化、教育、养老等)各领域被广泛应用，且与政府直接采购服务或特许经营等传统方式相比，PPP模式的应用更能缓解地方政府的财政支出压力，提高基建和公共服务的运营质量和效率，扩大社会资本的合理收益来源。而随着公众对“新基建”的需求越来越高，PPP模式的应用也将会从传统的基础设施、公共事业领域扩展到更为广泛的公共服务范围，包括ICT领域。

与传统基础设施项目最大的不同，ICT项目更加依赖于数字化技术，这些并不是地方政府或政府平台公司的核心能力，因此，需要由具备技术能力的社会资本采用市场化模式自行商业化实施，或者与地方政府合作实施，通过PPP模式共同参与到项目的投资、建设和运营管理中去，为政府解决数字化管理“补短板”难题，进一步提高公共信息处理和网络服务的运营质量和效率。同时，建立政企合作关系也能够实现促进当地科创产业发展、建立地方科技产业链的目的，进而让地区经济发展方式转型和产业升级步伐更为稳健。

SECTION 002

PPP-ICT项目交易结构设计要点——以A地区空间数据服务平台PPP项目为例

笔者参与的A地区空间数据服务平台PPP项目(以下简称“本项目”)是财政部第四批示范项目、国土资源系统首个PPP项目,该项目以空间数据服务平台为载体,以地理空间框架为定位基准,集成城市自然、社会、经济、人文、环境等综合信息,基于网络基础设施实现城市信息的广泛共享。该项目的成功落地,使得ICT与PPP的完美结合成为可能,也能为其他同类型项目提供参考模板。

1、综合考虑项目实际因素合理选择项目运作方式

在ICT项目运作方式的选择上,需综合考虑项目性质、风险分配基本框架、融资需求和期满处置等各项因素。实践中,该类型的PPP项目通常以BOT(建设-运营-移交)作为主要运作方式,由社会资本或项目公司承担新建项目的设计、融资、建设、运营、维护和用户服务职责,由政府方授予其在合作期限内的运营管理和收费权利,并在合同期满后项目资产及相关权利等移交给政府方。本项目即采用了典型的BOT运作方式,项目合作期限30年,其中建设期3年,对建设过程中形成的智慧城市“大数据资产”,投资人还将享有27年的运营权,这种“数据资产经营”模式将为投资人带来长期稳定的现金流。

另外,对于其他类型的ICT还可进一步考虑采用BOO(建设-拥有-运营)方式,即由社会资本或项目公司拥有项目所有权,政府方享有对社会资本的监督权利,并在合同中要求社会资本受到保证公益性的约束条件。同时,O&M(委托运营)也是国际上较为常见的运作方式,具体由政府将存量公共资产的运营维护职责委托给社会资本或项目公司,政府保留资产所有权,只向社会资本或项目公司支付委托运维费。

2、灵活运用市场化融资工具拓展项目建设资金来源

为缓解政府前期财政支出责任压力,项目前期的建设费用通常由社会资本负责筹措,具体由政企双方按照一定比例资本金出资到位,剩余所需资金依赖于银行贷款等债务性资金筹集,且PPP项目中又以项目融资为主,即以项目本身的现金流量、项目资产与合同权益等开展融资工作,政府或社会资本无需提供额外的担保增信措施。而为进一步拓展项目建设资金来源,实践中越来越多的PPP项目通过基金等结构化融资手

段完成投融资责任。如在本项目中,社会资本由设备供应商、运营维护商和产业投资基金三方组成联合体方式参与,在确保完成项目产出质量的同时解决了前段投资资金来源的问题,由基金方负责大部分资本金的筹集以及项目贷款的对接,通过在项目公司层面控股并取得运营期内的股权分红方式取得收益。

另外,2019年6月,中共中央办公厅、国务院办公厅印发《关于做好地方政府专项债券发行及项目配套融资工作的通知》,提到精准聚焦重点领域和重大项目,鼓励地方政府和金融机构依法合规使用专项债券和其他市场化融资方式,重点支持符合条件的重大项目建设。因此,在地方政府专项债加速发行、可作为重大项目资本金的背景下,将PPP与专项债结合,不仅降低了项目资金压力,而且还能形成政策合力,助力经济高质量发展。

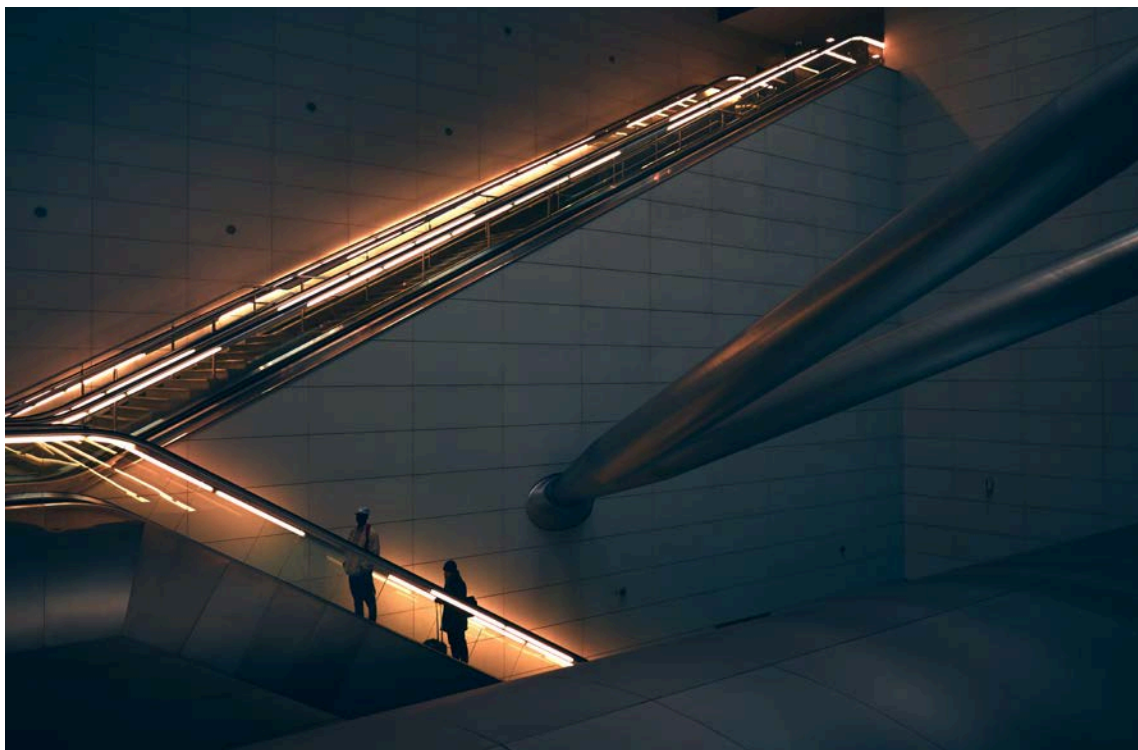
3、全面整理对信息和技术系统风险的识别和防范

在风险识别方面,由于ICT项目所具有的技术专业性和复杂性,除通常PPP项目所涉及的建设、运营、宏观政策和不可抗力风险等,还需单独考虑技术和信息系统风险。如面对服务需求不清晰和设计方案选择不当的风险,在项目实施初期应对项目需求进行详细调研,根据调研结果优化设计方案,同时充分考虑本项目实际情况,如子系统资源需求、子系统的制约关系、资源限制、项目总工期限制等因素,参考同类项目实施经验,制定切合实际的详细的项目基准计划,制定详细的项目实施方案。

又如,为应对系统开发质量缺陷和开发工作缓慢所可能导致的项目进度受阻以及建设成本不可控的风险,在项目实施过程中,应对项目质量、进度、投资等要素进行监控,敦促项目按计划进行,对于项目实施中出现的非预期情况进行分析,尽快采取恰当的措施进行处理,根据变更(项目范围变更、需求变更、方案变更、工期变更等等)调整基准计划,即对项目基准计划进行动态管理。同时,也可以选择具有大型信息化项目咨询和监理经验的项目监理公司,协助建设单位做好项目管理工作。

4、重视项目立项与审批风险保障项目全过程合规性

除对于信息和技术系统风险的识别和防范,由于ICT类项目所涉及的项目立项和审批环节众多,因此还应格外重视因项目前期立项或审批文件缺失所导致的合规性风险。具体而言,通常诸如数据处理或云计算中心项目的实施会以取得立项批复(政府审批、企业核准或备案)、节能评估和电力指标为前提要求,对于特殊领域,如提供互联网增值服务或内



容分发网络业务的, 还需取得IDC或CDN牌照。同时, 在项目实施过程中, ICT类项目还会涉及土地和厂房、环境影响评估、用电方案、消防设计审核或备案和竣工后相关验收等各个要素, 需特别注意各个要素缺一不可, 否则极可能会影响到项目的正常运营。

5、建立风险共担和激励相容机制的收益分配机制

ICT项目属于准经营性项目, 以本项目为例, 其经营收入可来源于信息化服务和数据中心档案室租金收入, 用户来自政府相关部门、企业、个人, 其中政府相关部门、企业是目前使用者付费的主要来源。在经营性收入不足部分, 由政府提供可行性缺口补助, 并由市县两级财政根据项目投资规模、各县市地籍测绘面积、人口数量、一般公共预算收入等实际情况共同分担。

但是, 考虑到市场风险的不可控可能导致项目实际运营收益低于预期, 影响到社会资本的合理收益水平和项目的可融资性, 针对该类准经营性项目, 可视情况设置最低需求量和超额收益回报机制来实现政企之间的风险共担、收益共享。具体而言, 可在合同中约定当实际经营收入小于预测收入时, 社会资本就其经营业务在一定范围(如50%)内自负盈

亏,当实际经营业务收入低于预测收入的50%时,政府就不足的差额收入部分予以补偿。相反,当实际经营收入大于预测收入时,政府也应享有一定比例的收益分成,分成比例可根据收益区间按阶梯比例设定。

6、借助第三方专业力量制定项目运营绩效考核机制

ICT项目运营质量和效率水平的高低决定了项目产出目标能否实现,以及政府和公众是否可以享有高质量的信息化公共服务,因此对于运营期内绩效考核设置的设定尤为关键。针对ICT等信息科技类项目,其考核的重点通常包括运维服务管理制度的规范(含服务时间、行为规范、现场服务支持和问题记录等)、网络和安全系统运维服务质量(含现场备件安装、现场软件升级、现场故障诊断和问题管理系统等)、软硬件设备的维修服务(含系统支撑软硬件的日常维护、服务器维护、存储设备维护、网络和安全设备维护和数据库系统维护等)和其他运维服务(含人员的技术培训服务、质量管理要求和项目管理要求等)多方面进行考核,以保证用户信息系统的正常运行,提高信息系统的整体服务水平。在具体实施过程中,由于ICT项目运维考核的专业性,双方可共同委托第三方制定绩效考核评分细则、开展绩效监测以及中期评估等。同时,根据项目进展情况,政企双方也可通过磋商机制适时修正及合理调整考核机制的指标和细则。

7、提供必要的政府支持与保障

PPP-ICT项目的顺利落地和实施离不开政企双方长效合作机制的建立以及政府方的支持与保障,包括项目前期审批和许可手续的办理,协调相关用户单位与社会资本签署支付协议,制定项目信息系统或设施的适用管理办法、明确用户收费标准以及将政府补助及时纳入年度财政预算及中期财政规划等等。

8、设置再谈判机制

考虑到较长的项目合作周期内所可能发生的客观情况变化,项目运营过程中后续约定服务标准、大修费用、市场情况、管理成本等可能会发生较大变化,为保障系统基本公共服务质量和效率,政企双方还应提前建立顺畅的沟通和再谈判机制,以确保社会公共服务的持续供给以及政企合作关系的长久稳固。

SECTION 003

结语

随着“新基建”的兴起和中央经济稳增长措施的不断出台,未来ICT领域内的PPP项目将会越来越多地走上舞台,“PPP+ICT”给PPP模式带来了新的内涵和应用空间。未来,政企双方如何在新兴领域实现长久和深入的合作值得业界的共同探讨,也离不开具体项目的不断实践和总结。另一方面,由于PPP-ICT项目仍属于创新性投资项目,在其实施过程中,各方应提前做好交易结构的设计工作,防范风险于未然。



周月萍/合伙人
房地产和基础设施部
上海办公室
+86 21 6061 3098
cindyzhou@zhonglun.com



周兰萍/合伙人
房地产和基础设施部
上海办公室
+86 21 6061 3766
laurazhou@zhonglun.com

参考文献:

- 1、《王守清:当智慧城市遇到PPP-ICT项目》,胡一石、王守清,2015年10月28日,载于项目管理评论微信公众号, <https://mp.weixin.qq.com/s/7q8AXswUPdToeD1fsz0whg>;
- 2、《当PPP遇上新基建,业内人士有话说!》,中国财经报,2020年3月16日,载于财政部PPP中心官网, <https://www.cpppc.org/PPP-yw/1371.jhtml>。



2

CHAPTER 02

中国自动驾驶行业的主要法律规制及实务

作者:丁恒/潘玲

2017年4月6日,工业和信息化部(以下简称“工信部”)、国家发展改革委、科技部在其发布的《汽车产业中长期发展规划》中提出了“到2020年,汽车DA(驾驶辅助)、PA(部分自动驾驶)、CA(有条件自动驾驶)系统新车装配率超过50%,网联式驾驶辅助系统装配率达到10%,满足智慧交通城市建设需求;到2025年,汽车DA、PA、CA新车装配率达80%,其中PA、CA级新车装配率达25%,高度和完全自动驾驶汽车开始进入市场”的目标,自动驾驶汽车产业在中国进入高速发展模式。在工信部、公安部、交通运输部于2018年4月12日联合发布了《智能网联汽车道路测试管理规范(试行)》之后,北京、上海、广州、重庆、江苏等地相继出台了关于自动驾驶汽车道路测试的地方规定,并陆续发放了道路测试牌照,湖北省武汉市更在2019年9月22日向包括百度在内的三家公司颁发了全球首批自动驾驶商用牌照。然而,虽然目前中国国内的自动驾驶行业发展如火如荼,但是该行业除了需要技术和大量资金外,在法律方面,比如测绘等方面仍然存在较高的门槛和不确定性。

随着5G的进一步普及,自动驾驶汽车将成为Mobility as a Service (“MAAS”)¹应用的重要一环。MAAS应用及自动驾驶汽车技术将大幅提高出行的便利度,并有效降低出行成本以及物流费用。而中国也预计成为MAAS应用与自动驾驶结合的最大的市场之一。中国市场的巨大发展潜力,吸引了不少外国投资者的目光。

根据现行有效的《外商投资准入特别管理措施(负面清单)》²(以下简称“负面清单”),自动驾驶系统的研发等不属于负面清单的范围。不仅如此,根据现行有效的《全国鼓励外商投资产业目录》³,自动驾驶控制系统的研发属于全国鼓励外商投资产业目录项下。因此,我们可以看出,从政策层面上,国家对于外资企业投资自动驾驶领域是持欢迎甚至鼓励态度的。但是,这并不意味着外国投资者进入中国的自动驾驶领域就畅通无阻了。实践中,外国投资者在中国布局自动驾驶产业,测绘及电信等方面仍然面临法律上的限制。

本文主要从测绘、电信管理以及数据安全角度简要分析自动驾驶行业涉及的法律规制与相关的主要问题。

SECTION 001

测绘相关法律规制

1. 自动驾驶领域的主流定位方式

对于自动驾驶汽车来说,其最重要的技术核心在于使得汽车能够实时获取汽车自身定位并对汽车在周围环境中的相对位置进行认知。从目前来看,在自动驾驶领域中,针对自动驾驶技术中的核心定位技术,有两种主流方式。

(1) 以Waymo为代表的高精地图定位

此种方式主要是指通过激光雷达,将激光雷达实时获取的周边信息反映到预制的高精地图上,将实时信息与高精地图中的已有信息进行比较,判断路况是否发生改变,并以此实现在该高精地图涵盖范围内的自动驾驶。

此种方式是目前自动驾驶汽车企业所广泛采用的一种主流定位方式。

(2) 以特斯拉为代表的SLAM定位方式

此种方式主要是指通过配置的传感器,实时获取路面路况信息,并通过该路面路况信息实时构建地图。其与高精地图定位方式的最大差别就在于SLAM定位不需要预先录入高精地图。

1. MAAS,根据交通运输部于2019年7月25日印发的《数字交通发展规划纲要》,意为“出行即服务”,是指以数据衔接出行需求与服务资源,使出行成为一种按需获取的即时服务。

2.《外商投资准入特别管理措施》2019年版。国家发展和改革委员会、商务部2019年6月30日发布。(文号:中华人民共和国国家发展和改革委员会、中华人民共和国商务部令25号)

3.《全国鼓励外商投资产业目录》2019年版。国家发展和改革委员会、商务部2019年6月30日发布。(文号:中华人民共和国国家发展和改革委员会、中华人民共和国商务部令27号)

2. 定位方式导致的测绘相关法律规制

对自动驾驶汽车来说,无论通过上述哪一种定位方式,在自动驾驶过程中,自动驾驶汽车均需要通过车身自带的激光雷达或传感器,实时捕捉道路信息、路况信息,并将这些信息实时传输至终端,通过终端进行计算、验证并最终反馈至车辆以达到控制车辆并作出有效驾驶决策的目的。而这一过程,可能会被认为属于测绘行为。

出于国家安全等原因,在中国,对于测绘行为,一直存在较为严格的限制,不同的测绘业务需要取得不同级别的测绘资质。同时,在这一领域,也一直有着明确的外商投资限制。

根据《关于加强自动驾驶地图生产测试与应用管理的通知》(国测成发[2016]2号) (“通知”)的规定,自动驾驶地图属于导航电子地图的一种,其数据采集、编辑加工和生产制作必须由具有导航电子地图制作测绘资质的单位承担,不仅如此,在导航电子地图制作单位与汽车企业合作开展自动驾驶地图的研发测试时,必须由导航电子地图制作单位单独从事所涉及的测绘活动。同时,通知还要求,对于道路测试的地图数据(包括在传统导航电子地图基础上增添内容、要素或精度提升的),需要按照涉密测绘成果进行管理,并采取有效措施确保数据安全,未经省级以上测绘地理信息行政主管部门批准,不得向外国的组织和个人以及在中国注册的外商独资和中外合资、合作企业提供、共享地图数据。

然而,尽管有上述规定,对于自动驾驶企业在提供自动驾驶服务的过程中是否需要取得测绘资质以及如果需要,则应取得怎样的测绘资质,目前法规没有明确规定。

笔者认为,自动驾驶企业在自动驾驶过程中通过激光雷达或传感器实时采集信息的行为是否属于测绘,取决于该自动驾驶企业在开展自动驾驶业务时,其与地图服务提供商的具体业务模式以及是否参与采集地理信息。

一般来说,自动驾驶企业在中国开展自动驾驶业务时,对于地理信息采集,存在如下两种模式。

(1) 模式①

车辆采集的地理信息将实时传输至自动驾驶企业,由自动驾驶企业将信息交给地图服务提供商处理,地图服务提供商在处理完相关数据后,将数据传输回自动驾驶企业,最终由自动驾驶企业将信息反馈至车辆。此外,自动驾驶企业利用地图服务提供商提供的精准地图,为自动驾驶汽车提供导航服务。

如果采用该种模式,那么该自动驾驶企业的行为就涉及地图数据的采集,属于《中华人民共和国测绘法》(以下简称“《测绘法》”)第2条所定义的测绘行为。根据《测绘资质分级标准》,该自动驾驶企业实施的行为有很大可能属于地面移动测量、导航电子地图制作或者互联网地图服务。

而根据负面清单,地面移动测量以及导航电子地图制作都属于禁止外商投资的项目。而互联网地图服务虽然不属于禁止外商投资的项目,但是,根据《外国的组织或者个人来华测绘管理暂行办法》第6条的规定,外国的组织或者个人在中华人民共和国领域测绘,必须与中华人民共和国的有关部门或者单位依法采取合资、合作的形式。

(2) 模式②

车辆直接将采集到的地理信息传输给地图服务提供商,由地图服务提供商在处理完成该信息后,直接反馈至车辆。在此模式下,自动驾驶企业全程不参与信息采集,仅提供自动驾驶方案。

如果自动驾驶企业采用该模式,鉴于该公司不会参与到采集地理信息、处理地理信息的过程中去,笔者基本认为自动驾驶企业无需取得测绘资质。

据悉,国家测绘管理局正在修改测绘资质相关的文件,预计在不久的将来,对于自动驾驶行业所涉及的测绘资质会进行明确的规定。笔者建议自动驾驶企业持续关注该立法动态。

SECTION 002

电信业务方面规制

1. MAAS应用

MAAS旨在构建“出行者将出行视为服务,依据自身不同的出行需求,购买运营商提供的出行服务”这一应用场景。

在此理念下,自动驾驶出租车预计将成为该应用场景的重要一环。而为了连接起出行客户与自动驾驶汽车,就需要构建一个网络平台,实时将客户的需求传输至自动驾驶汽车的终端。

2. 自动驾驶过程中所涉及的电信业务规制

自动驾驶车辆实时收集信息上传到自动驾驶企业的平台,经自动驾驶企业处理之后,再次反馈给自动驾驶车辆的行为,无论是在目前还是将来成为MAAS应用的一环,通过网络平台将客户的出行需求传输到自

4.根据《电信业务分类目录》的定义,在线数据处理与交易处理业务是指:在线数据处理与交易处理业务是指利用各种与公用通信网或互联网相连的数据与交易/事务处理应用平台,通过公用通信网或互联网为用户提供在线数据处理和交易/事务处理的业务。在线数据处理与交易处理业务包括交易处理业务、电子数据交换业务和网络/电子设备数据处理业务。

5.信息服务业务是指通过信息采集、开发、处理和信息平台的建设,通过公用通信网或互联网向用户提供信息服务的业务。信息服务的类型按照信息组织、传递等技术服务方式,主要包括信息发布平台和递送服务、信息搜索查询服务、信息社区平台服务、信息即时交互服务、信息保护和处理服务等。

自动驾驶汽车终端,都不可避免地会涉及到相关增值电信业务方面的服务。

根据《电信业务分类目录》,自动驾驶车辆收集信息并向车辆反馈信息的行为,一般涉及到《电信业务分类目录》中的B21项在线数据处理与交易处理业务⁴及B25信息服务⁵。

根据负面清单,增值电信业务的外资股比不应超过50%(电子商务、国内多方通信、存储转发类、呼叫中心除外)。

同时,根据《中华人民共和国电信条例》第9条,经营增值电信业务,业务覆盖范围在两个以上省、自治区、直辖市的,须经国务院信息产业主管部门审查批准,取得《跨地区增值电信业务经营许可证》;业务覆盖范围在一个省、自治区、直辖市行政区域内的,须经省、自治区、直辖市电信管理机构审查批准,取得《增值电信业务经营许可证》。

因此,自动驾驶企业应取得相应的增值电信业务经营许可证,同时,需要留意外资股比不得超过50%的限制。不仅如此,自动驾驶企业应根据其将来开展的业务内容,判断其是否需要获得其他电信业务项下的资质,并及时取得该等资质。

SECTION 003

数据安全、信息跨境传输及隐私相关风险

随着2016年《中华人民共和国网络安全法》(以下简称《网络安全法》)的实施,网络安全、数据安全已经变成各企业合规工作的一环。根据《网络安全法》第2条及第76条规定,在中国境内建设、运营、维护和使用网络的行为,以及作为网络的所有者、管理者或网络服务提供者的网络运营者均适用《网络安全法》。

由于《网络安全法》的法条对网络运营者的规定比较宽泛,因此,即使是使用公司内部局域网进行数据处理,我们也倾向性认为其属于网络运营者。作为自动驾驶企业来说,不可避免地一定会使用网络进行数据分析及数据储存,因此,自动驾驶企业属于《网络安全法》规定的网络运营者。同时,鉴于自动驾驶企业收集的数据涉及交通信息以及大量个人信息,因此,也很有可能被认为属于关键信息基础设施的运营者。有鉴于此,自动驾驶企业必须遵守《网络安全法》及其相关的法律法规。随着近年来中国对于数据安全的日益重视以及监管的日趋严格,笔者建议企业及时制定数据合规管理制度,降低数据合规风险。

另一方面,对跨国自动驾驶企业来说,可能倾向于将自动驾驶测试过程中的相关测试数据、软件数据、实时数据同步存储至国外服务器上,而这一行为,会涉及到数据的跨境传输。根据《网络安全法》第37条的规定,“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要,确需向境外提供的,应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估;法律、行政法规另有规定的,依照其规定。”因此,若涉及关键信息基础设施的运营者的数据跨境传输,企业应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。关于数据出境评估的具体规定,如《个人信息和重要数据出境安全评估办法(征求意见稿)》、《信息安全技术 数据出境安全评估指南(征求意见稿)》、《个人信息出境安全评估办法(征求意见稿)》等都处于意见征求阶段,尚未正式实施。根据《个人信息出境安全评估办法(征求意见稿)》,即使不是关键信息基础设施的运营者,其他网络运营者跨境提供个人信息时,也需要进行安全评估。因此,笔者建议企业关注将来立法动向,一旦相关法规实施,就立刻采取相应措施,切实履行相关规定。

此外,自动驾驶汽车在行驶过程中,其所配备的传感器或摄像头不可避免地会拍摄到行人人脸等个人信息。根据《网络安全法》第76条规定及《信息安全技术 个人信息安全规范》(以下简称《个人信息安全规范》),人脸为个人生物识别信息,属于个人敏感信息。根据《网络安全法》、《个人信息安全规范》的相关规定,获取个人的面部特征需获得相关个人的明确同意。但是,考虑到实践中取得每个行人个人的同意是不现实的,自动驾驶企业如何在提供自动驾驶服务的过程中遵守该规则,还需要进一步探讨以及关注立法动向。



丁恒/合伙人
公司一部
上海办公室
+86 21 6061 3736
dingheng@zhongtun.com



3

CHAPTER 02

高精地图产业法律问题

作者:邱建/朱永春/陶媛园/陈嘉琳/王丹

高精地图,也称为高精度地图(High-Definition Map,简称HD Map),通常指专为自动驾驶制作的地图。传统导航地图精度只有5到10米,而高精地图精度可高达厘米级,常为自动驾驶系统提供所需信息。自动驾驶系统根据高精地图所提供的信息进行实时判断并定位。今年来,自动驾驶已成为车企和多领域科技公司共同抢占的潮头,作为支持自动驾驶技术落地的关键环节,高精地图的重要性不言而喻。结合实践经验,本文旨在探讨高精地图产业的相关法律问题。第一部分重点分析进入高精地图产业的重要“门槛”,第二部分将围绕外国投资者进入高精地图行业的障碍及可行途径进行探讨,第三部分就高精地图涉及的数据安全问题,从数据采集、储存、传输、发布等多个环节进行讨论。最后在第四部分,我们拟对众包模式的概念、现状以及存在的法律问题等方面进行讨论,供读者参考。

PART 1

导航电子地图资质

SECTION 001

何为高精地图？

与传统的导航地图(Street Directory Map, 简称SD Map)不同, 高精地图提供车道级别信息(Lane level info), 精度高达厘米级, 其路径规划称作局部路径规划(Planning)。按级别和精度的不同, 高精地图可分为ADAS(Advanced Driver Assistance System, 高级驾驶辅助系统)地图和AD(Autonomous Driving, 自动驾驶)地图, 以结合不同精度要求对应不同的智能驾驶需求。传统导航地图与ADAS地图、AD地图的对比如下表所示:

要素	传统导航地图	高精地图	
		ADAS地图	AD地图
地图信息	道路级别信息 (Road Level Info)	车道级别信息 (Lane Level Info)	
路径规划	全局路径规划(Routing)	局部路径规划(Planning)	
精度	5到10米	米量级	厘米量级
信息量	道路级别数据: 道路形状、坡度、铺设、方向等	高精道路级别数据: 道路形状、坡度、曲率、铺设、方向等	增加车道属性相关数据以及高架物体、防护栏、树、道路边缘类型、路边地标等大量目标数据
实时性	永久静态数据(更新频率约1个月), 半永久静态数据(更新频率约1小时)	永久静态数据(频率约1个月), 半永久静态数据(频率约1小时), 半动态数据(频率约1分钟), 动态数据(频率约1秒)	
街道名称信息重要性	重要	一般	一般
道路曲率数据重要性	一般	重要	重要
道路几何特征	重要	重要	重要
使用对象	驾驶员	面向机器, 供智能驾驶汽车使用	
定位	依赖GPS定位, 定位准确性取决于GPS精度、信号强弱及定位传感器的误差	通过更高维数的数据结合高效率的匹配算法, 能够实现更高尺度的定位与匹配	
功能	辅助驾驶的导航功能	"地图匹配+辅助环境感知+路径规划": 通过"高精度+高动态+多维度"的地图数据为智能驾驶提供自变量和目标函数	

1. 国家测绘地理信息局(现已合并到自然资源部)于2016年2月3日颁布《关于加强自动驾驶地图生产测试与应用管理的通知》。

从地图数据上来看,高精地图数据的精度更高、维度更多,兼有静态要素(如道路交通基础设施、车道网和道路网等)和动态要素(如道路拥堵情况、交通事故等)。其主要分为两类:一是道路信息,包括高速公路等车道的位置、类别、宽度、坡度和曲率等信息;二是与车道相关的附属设施及构造物等信息,包括交通标志、交通信号灯、过街天桥、交通监视点(电子眼、测速雷达)、路侧设施、障碍物等道路细节和基础设施信息,并特别包括车道限制场景(如车道上某一时段限行)和车道限制信息(如车辆类型、天气状况、通行时间)等。

通过这些数据,自动驾驶车辆的导航系统可以完成准确定位,判断哪些道路可以行驶,为车辆提供指引。

SECTION 002

何谓导航电子地图资质?

根据我国《测绘法》的定义,测绘活动系指“对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述,以及对获取的数据、信息、成果进行处理和提供的活动”。如上文所述,高精地图的制作涉及大量与地理要素和地表人工设施有关的数据采集、编辑加工和生产制作等活动,因此该等活动极可能被视为测绘活动。

根据《测绘法》,我国对从事测绘活动的单位实行测绘资质管理制度。进一步地,根据原国家测绘地理信息局(现已合并到自然资源部)相关规定,高精地图(即该通知所称“自动驾驶地图”)属于“导航电子地图的新型种类和重要组成部分”,并且自动驾驶地图的“数据采集、编辑加工和生产制作必须由具有导航电子地图制作测绘资质的单位承担”¹。

通常,测绘资质分为甲、乙、丙、丁四级,其专业范围分为大地测量、测绘航空摄影、摄影测量与遥感、地理信息系统工程、地图编制、导航电子地图制作、互联网地图服务等。但是,对于导航电子地图制作测绘资质,目前仅有甲级测绘资质,没有其他等级。我们在本系列文章中所讨论的“导航电子地图资质”即指导航电子地图甲级测绘资质。

SECTION 003

谁需取得导航电子地图资质?

从《测绘法》、《关于导航电子地图管理有关规定的通知》和《关于加强自动驾驶地图生产测试与应用管理的通知》等的规定来看,需取得导航

2. 国家测绘地理信息局(现已合并到自然资源部)于2014年7月1日颁布《测绘资质分级标准》。

3. 注册测绘师,是指经过考核认定和注册测绘师资格考试取得《中华人民共和国注册测绘师资格证书》,并依法进行注册的人员。注册测绘师可以计入中级专业技术人员数量。

4. 《测绘资质管理规定》第二十三条:测绘资质年度报告内容包括本单位符合测绘资质条件、遵守测绘地理信息法律法规、上一年度单位名称、注册地址、办公地址和法定代表人变更、专业技术人员流动、仪器设备更新、基本情况变化(含上市、兼并重组、改制分立、重大股权变化等)、测绘地理信息统计报表报送情况、测绘项目质量(用户认可或者通过质检机构检查验收)、诚信等级等情况。

电子地图资质的测绘活动包括导航电子地图数据的采集、编辑加工、格式转换和地图质量测评等。

但是,上述法规并未明确界定何谓导航电子地图数据。根据《GB/T 28442-2012_导航电子地图数据分类与编码》,我们理解,导航电子地图数据系指“含有空间位置地理坐标,能够与空间定位系统结合,准确引导人或交通工具从出发地到达目的地的电子地图或数据集”之相关数据。尽管如此,对于路况信息、交通标志、树木、障碍物、坑洼、建筑物、道路维修信息、交通事故等信息,是否一概被视为导航电子数据,并无定论,尤其是该等信息并未与GPS等定位信息相绑定时。实践中,虽然自然资源部倾向于较为严格地认定该等信息属于测绘数据(不论是否包含GPS定位信息),我们也注意到有观点认为,如果采集的数据不包含GPS等定位信息,则该等数据不属于测绘数据,相应的数据采集及后续的编辑、加工等行为亦不视为测绘活动,因而也无需取得导航电子地图资质。

此外,需要指出的是,根据《关于导航电子地图管理有关规定的通知》,除依法取得导航电子地图资质者外,其他单位和个人在使用高精地图过程中,不得携带其他带有空间定位系统(如GPS等)信号接收、定位功能的仪器开展显示、记录、存储、标注空间坐标、高程、地物属性信息,以及检测、校核、更改高精地图相关内容等测绘活动。就此问题,笔者在后续探讨“众包模式”的文章中会进一步讨论。

SECTION 004

如何取得导航电子地图资质?

实践中,取得导航电子地图资质的方式主要有如下两种:(1)自主申请;(2)收购具有资质的单位。

根据《测绘资质分级标准》²规定,申请导航电子地图资质的企业需达到以下两方面的标准:(1)适用于各测绘资质的通用标准:包括主体资格、专业技术人员、仪器设备、办公场所、质量管理、档案和保密管理、测绘业绩以及测绘监理共8个方面的原则性要求;(2)仅适用于导航电子地图资质的专业标准:主要包括人员规模、仪器设备、保密管理和作业标准共4个方面的要求。其中,测绘及相关专业人员应达到100人(含注册测绘师5人³),其中至少包括高级10人、中级20人;同时,专业技术人员还需满足学历标准、相关岗位的工作年限以及取得任职/职业资格的要求。此外,由于我国实行测绘资质年度报告公示制度⁴,测绘资质企业需要持续性地达标才能维系其导航电子地图资质,否则可能面临丧失导航电子地图资

5.《测绘资质管理规定》第三十条:测绘资质单位的部分专业范围不符合相应资质标准条件的,应当依法予以核减相应专业范围。

质的严重后果⁵。因此,实践中,申请和维持导航电子地图资质的难度和成本都非常高。公开资料显示,截至目前,仅22家企事业单位取得了导航电子地图资质(具体见附件)。从审批趋势上来看,自2001年四维图新获得第一张导航电子地图资质后,截至2018年末的18年间仅有16家单位拿到该资质,平均每年不足1家。而2019年一年间新增5家企业,2020年首月又新增1家企业。

近年来,由于自动驾驶、机器人配货、智慧城市等需要导航电子地图支持的产业日益兴起,众多科技巨头或汽车厂商也纷纷瞄准高精地图行业、意图布局该领域。鉴于自主申请导航电子地图资质的难度较大,不少企业也选择以收购持有导航电子地图资质的企业的方式间接获取这一资质。例如,阿里巴巴集团2013年5月入股高德地图(持股28%),2014年2月全资收购高德地图;腾讯2014年1月全资收购大地通途,同年5月收购四维图新11.28%股权;百度2013年全资收购长地万方等。需要注意的是,测绘资质企业在年度报告中需要对自身基本情况变化(包括兼并重组、重大股权变化等)进行公示,并应对测绘资质年度报告的真实性、合法性负责。若主管部门认为企业的股东方存在准入问题(例如涉及外资),则不排除主管部门在年度审核时对企业资质提出质疑乃至撤销。因此,如拟以收购方式获取导航电子地图资质,收购方应在尽调中对资质的有效性(特别是针对目标企业拥有的测绘人员、设备、保密制度、作业标准等对于维系资质至关重要的因素)进行重点核查,并对股东变更是否影响资质予以慎重评估。

SECTION 005

立法动态观察

虽然近年来取得导航电子地图资质的企业有所增加,但这是否意味着导航电子地图资质政策有所放宽呢?从立法动态变化来看,似乎并非如此。

去年5月,中国地理信息产业协会受自然资源部国土测绘司委托,面向协会相关会员单位征求对《测绘资质管理办法(征求意见稿)》(“征求意见稿”)的意见建议。与现行的《测绘资质管理规定》和《测绘资质分级标准》(“现有规定”)相比,征求意见稿提议了以下变化:

(1)增设“乙级”资质:征求意见稿拟在导航电子地图资质项下增设“乙级”资质。持有乙级资质的企业仅可在具体的省级范围内从事有关测绘活动,不得承揽跨省项目。由于高精地图大多旨在获取跨省地理信息,

因此乙级资质的作用相对有限。

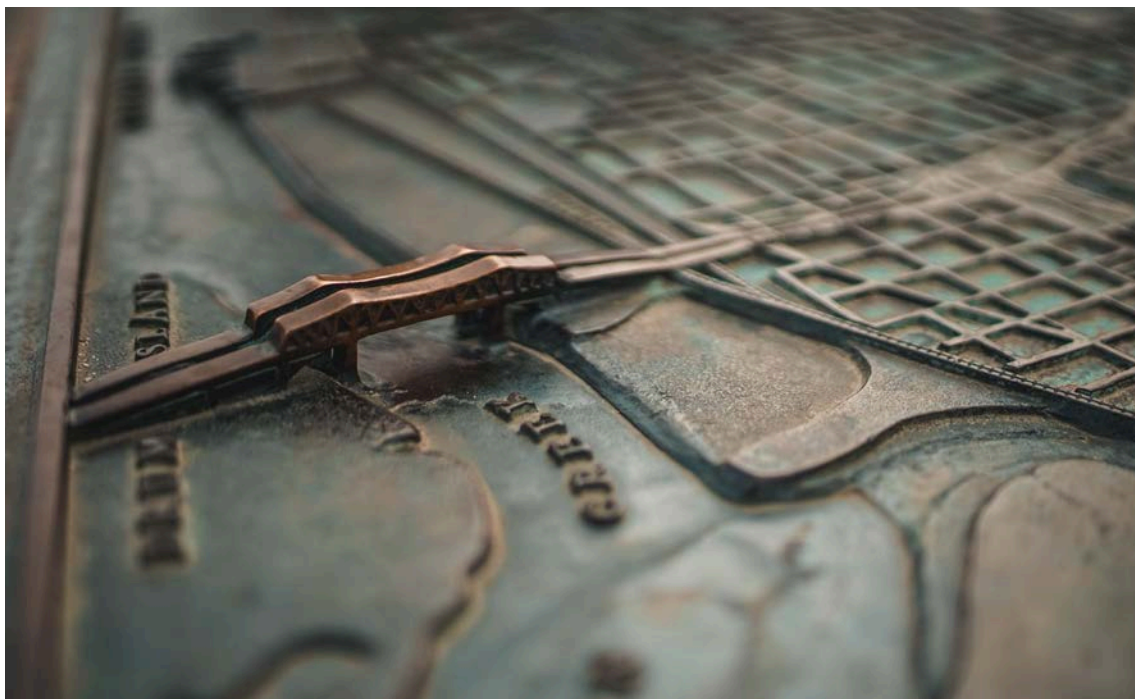
(2)改变专业人员数量要求:在导航电子地图甲级资质人员数量要求上,虽然征求意见稿拟在现有规定的基础上取消注册测绘师人数要求、降低测绘专业高中级人数要求,但拟要求更多的初级专业技术人员。

(3)增加申请“甲级”资质的前置要求:征求意见稿拟议,申请导航电子地图甲级资质的,应当取得乙级资质满2年、且所申请的每个业务范围近2年测绘服务总值不少于600万元(每个项目不低于50万元)。而现有规定则无上述年限和测绘业绩要求。因此,如征求意见稿的拟议规定被最终认可,导航电子地图资质的申请难度似乎比在现有规定下还要有所增加。

SECTION 006

小结

高精地图作为自动驾驶的底层设施之一,对这一领域的开拓者有着重要意义,而导航电子地图资质又是从事高精地图相关业务活动的前置“门槛”。鉴于该资质在取得、维系方面的难度和成本要求,有意进军自动驾驶领域的企业需要根据自己的业务模式和技术路线,审慎评估是否应取得这一资质、以及通过何种方式取得和维持这一资质(如该资质为其业务所必需)。



PART II

外资准入

2020年2月,发改委、工信部、自然资源部等11部委联合发布了《智能汽车创新发展战略》,提出到2025年要实现有条件自动驾驶的智能汽车规模化生产、高度自动驾驶的智能汽车在特定环境下市场化应用的战略愿景。潜力巨大的中国市场成为从业者必争之地,而高精地图产业作为自动驾驶产业链的上游也受到高度关注。但是,由于准入限制等原因,外国投资者进入中国高精地图行业存在诸多限制。围绕外国投资者进入高精地图行业的障碍及可行途径有哪些,是我们此部分关注的焦点。

SECTION 001

高精地图领域对外资的限制

按照我国现行法律法规,高精地图相关的数据收集、编辑加工、生产制作、格式转换等活动很可能被视为测绘范围内的导航电子地图编制活动。如果企业拟从事上述活动,应事先取得导航电子地图甲级测绘资质(“导航电子地图资质”)。此外,即使未直接开展前述活动,而仅在使用导航电子地图的过程中,通过带有空间定位系统(如GPS等)信号接收、定位功能的仪器收集有关坐标、地物属性信息(例如通过可定位的),或检测、更改导航电子地图的相关内容,根据有关规定亦需获得前述资质。

在高精地图的数据采集、编辑、加工等过程中,往往涉及对我国敏感目标的地理坐标、影像等数据的收集与处理,而该等信息多被视为国家秘密。若由外方接触和掌握该等战略性资源信息,可能从多方面对我国整体安全构成严重危害⁶。因此,历年以来,我国对外资进入这一领域均设置有严苛的准入限制。根据国家发改委、商务部颁布的《外商投资准入特别管理措施(负面清单)(2019年版)》,我国禁止外商投资“导航电子地图编制”领域。测绘领域的行业主管部门也对外资加以了严格的限制。《外国的组织或者个人来华测绘管理暂行办法》中要求,外国的组织或者个人在我国领域测绘,原则上必须与我国有关部门或者单位依法采取合资、合作的形式;但即使如此,合资、合作测绘项目仍不得涉足导航电子地图编制业务。

因此,根据目前的法规和政策,外国投资者无法单独或与境内机构合资合作取得导航电子地图资质,因而也无法在境内开展受制于资质许可的高精地图测绘相关业务。

6. 根据国家测绘地理信息局于2012年4月16日发布的《关于进一步加强导航电子地图数据保密管理工作的通知》,未经省级以上测绘地理信息行政主管部门保密技术处理的导航电子地图数据属机密级国家秘密资料。

SECTION 002

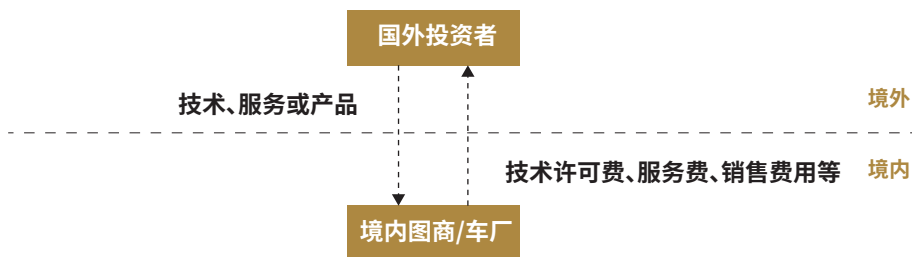
外资参与高精地图行业的路径分析

读到这里，读者们可能会心生疑惑。按照上文的说法，外资似乎无法进入我国高精地图行业，但近年来这一行业中似乎频频见到外资身影——荷兰导航及地图服务商TomTom与百度联手研发高精地图、高精度地图供应商HERE与四维图新设立合资企业、研发提升高精地图产品质量、某境外知名工业集团与高德等境内图商合作共同开发高精度地图等新闻不断抓住人们眼球。那么，这些“外国选手”是如何进入这一赛道的呢？

依照公开渠道的信息，我们试对外资参与境内高精地图业务的若干模式梳理、分析如下：

1. 跨境业务合作模式

外国投资者可以选择不在我国境内设立任何实体，而与境内拥有相应资质的公司达成跨境业务合作。在这种合作模式下，外国投资者可以向境内合作方提供技术、服务或产品，并从境内合作方收取服务费、许可费等。其合作模式如下图所示：



如上文介绍，外国投资者在境内开展高精地图相关业务高度受限。因此外国投资者与境内实体的合作分工应根据法律规定明确定位。例如，境外公司扮演技术、服务提供者的角色，不参与中国境内的测绘活动，而相应的有关数据的收集及高精地图的编辑、加工等活动仅由具有资质的境内公司负责。

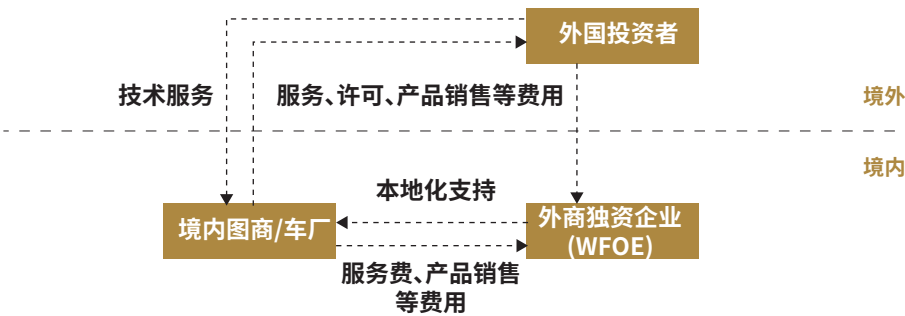
通过跨境业务合作，外国投资者一定程度上能够进入中国市场，并且在知识产权和商业秘密保护、资金投入等角度保有相当的灵活性。但是，这一模式整体来讲有不少弊端，例如：外国投资者无法独立在境内开展任何经营活动（因为在中国境内没有设立经营实体）；外国投资者对境内商业和文化环境、客户、技术信息等的远程了解和利用程度有限，常常出

现水土不服,也无法真正扎根中国市场;外国投资者和境内合作者的收入分配因涉及外汇监管、国际税收等事宜也较为复杂。此外,合作双方之间仅有合同关系,并无股权等资本纽带,合作的确定性、持续性和深度也大打折扣。

2. WFOE业务合作模式

考虑到跨境业务合作模式的种种弊端,不少外国投资者也尝试在境内设立外商独资企业(“WFOE”),通过WFOE与境内公司开展业务合作。与跨境业务合作模式相比,WFOE业务合作模式在合作收入结算上无需考虑外汇监管和国际税收程序。并且,WFOE作为中国境内企业,可以在中国招兵买马,获取第一手的市场信息、客户信息和技术信息并进行本地化利用,有利于提升竞争力。当然,由于在境内设立WFOE需要较多的资金投入并承担本地运营风险和成本,外国投资者往往先通过跨境业务合作试水,在对中国市场有一定了解后再逐步评估设立WFOE进行本地化合作的可行性。

实践中,出于保护关键技术和商业秘密等考虑,这一合作模式也常常与跨境业务合作模式组合运用——即WFOE在本地研发、服务支持及市场拓展等方面与境内合作伙伴合作,而由外国投资者跨境提供关键技术许可等。



需要指出的是,对外国投资者而言,WFOE模式虽然在本地化和合作深度、广度上有所进步,但这一模式依然受到外资准入和导航电子地图资质的监管限制,WFOE并不能从事导航电子地图的数据采集、地图制作、编辑等测绘业务。

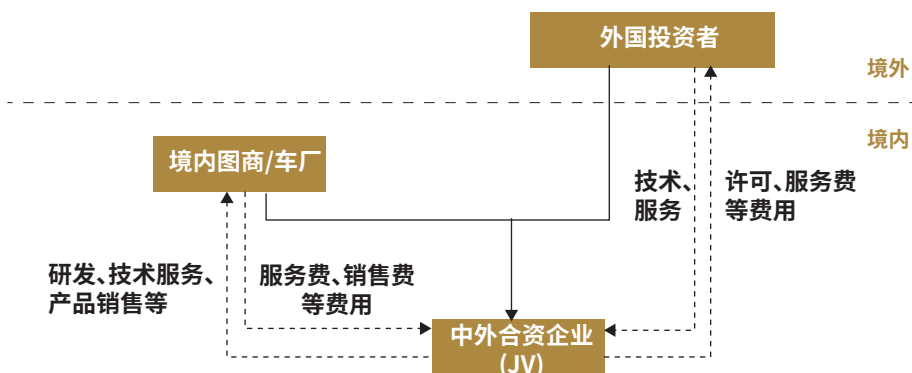
3. JV合作模式

在上述两种模式之外,也有外国投资者选择与境内合作伙伴共同设

7.国家测绘地理信息局于2016年2月3日发布的《关于加强自动驾驶地图生产测试与应用管理的通知》、于2007年11月19日发布的《关于导航电子地图管理有关规定的通知》等规定强调,用于自动驾驶技术试验、道路测试的地图数据(包括在传统导航电子地图基础上增添内容、要素或精度提升的),应当按照涉密测绘成果进行管理;不得向外国组织和个人以及在我国注册的外商独资和中外合资、合作企业提供、共享地图数据,不得在相关技术试验或道路测试中允许超出范围的人员接触地图数据。

8.在VIE架构下,境外实体能够通过其间接全资拥有的境内外商独资企业控制拥有相关业务资质的境内运营公司,并在一定程度上实现外资实际参与有关受限行业经营活动的效果。

立中外合资企业(“JV”),通过股权纽带加深双方合作。在JV合作模式下,双方利益进一步绑定,有助于整合境内外优势资源、发挥协同效应,甚至可借力于中国资本市场。在高精地图领域,境外图商等外国投资者与持有导航电子地图资质的国内图商设立JV已有先例。例如,HERE与四维图新于2017年合资成立北京图新瀚和科技有限公司,双方出资比例均为50%。根据公开信息显示,该JV从事的业务主要包括就自动驾驶进行研发、提升高精度地图的产品质量、客户推广等。

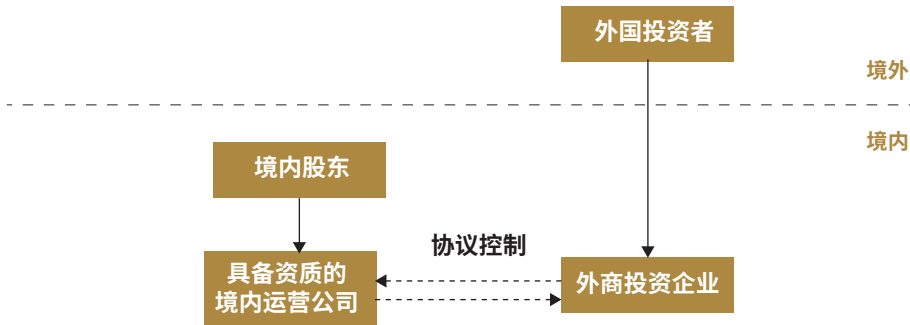


虽然我国允许外资以JV形式有限度地参与部分限制外商投资领域(例如医疗、通用航空、市场调查等),但在高精地图这一禁止外商投资领域,JV亦不能进入。因此,JV和WFOE一样,只能在法律法规允许的范围内提供研发、市场开拓等支持类服务,不得从事测绘活动。上文提及的图新瀚和为例,其经营范围并不包括测绘业务,亦未取得任何测绘资质,其开展的活动也限于有关支持类服务。

综合上述三种模式分析,不难发现,目前虽然外资在尝试以种种模式进入我国高精地图市场,但其本质仍限于研发、支持性技术服务和一定商业合作等,从而间接获得与中国高精地图市场有关的部分利益。有关数据采集、编辑、加工、制备等测绘活动仍由境内资质主体独立完成。对于在中国境内开展测绘活动、以及通过与境内实体合作获得或接触境内地图数据信息(尤其是数据出境)等⁷,在当前仍属不得跨越的红线。

4. VIE架构

VIE架构,也即协议控制模式,作为一种解决法律监管与商业诉求之间矛盾的权宜之计,在不少限制/禁止外商投资的领域内被广泛运用⁸。



9. 其VIE架构似乎在一定调整(如高德软件之股东发生调整)后仍得以保留。

在高精地图这一高度管控的领域，也不难发现VIE架构的身影。例如，高德软件有限公司（“高德软件”）于2004年6月取得了导航电子地图制作甲级测绘资质。根据我们在全国企业信用信息系统中进行的查询以及对AutoNavi Holdings Limited（“高德控股”，原NASDAQ:AMAP，现已退市）公告等公开信息的审阅，高德控股并不持有高德软件的股权，而是通过协议控制方式在高德软件的财务和运营决策等方面实现了控制。该等安排（及高德控股在纳斯达克上市）并未影响高德软件继续持有导航电子地图资质。2014年7月，高德控股私有化退市，成为阿里巴巴（已于美国纳斯达克及香港上市）旗下的全资子公司⁹，但是，高德软件持有的导航电子地图资质依旧未受到此次控制权变更的影响。

国内的其他互联网巨头公司也普遍采用这种架构安排参与到了这场高精地图的竞争中，例如北京长地万方科技有限公司（其于2013年被百度收购，百度已于纳斯达克上市）等；此外，根据我们在公开渠道的检索，北京初速度科技有限公司（“初速度”）等自动驾驶公司可能也采取了VIE架构。

上述先例的出现是否意味着，外国投资者也可利用VIE架构突破现有监管限制、从事高精地图相关活动呢？笔者认为，答案并非如此。无论是阿里巴巴、百度等领先互联网企业，还是初速度等初创公司，究其本质，其仍为扎根于国内的境内企业（主要股东和实际控制人仍属境内人士），与实控人和主要股东为境外人士的外商投资企业或者外国投资者相比还是有实质区别的。在限制/禁止外商投资领域，过去不乏外国投资者试图利用VIE结构进入相关行业、后被主管部门叫停的先例。鉴于高精地图相关测绘数据在安全方面的重要性，这一领域内外国投资者通过VIE架构绕过监管限制的可行性极低。

另一方面，从行业主管的过往实践来看，自然资源部对持有测绘资质的境内资质主体的股东背景一向予以高度关注。根据有关规定及实操要

10.采用VIE架构的企业须向自然资源部如实披露有关信息,并在年度报告中持续进行报备。

11.自然资源部实践中也具体关注有关协议条款的约定内容,若外方能够通过协议安排控制境内资质主体的业务、人事等业务相关方面,或能够以其他方式涉及参与测绘活动管理、接触测绘数据,则自然资源部将不予批准其申请;对于已取得导航电子地图制作甲级测绘资质的企业,前述情形不仅将导致有关资质将被取消,该企业亦可能面临处罚。

求,若资质主体采取VIE架构,不仅须向自然资源部如实披露有关信息¹⁰,也必须确保协议控制安排下外方的控制不会导致外方直接参与测绘活动管理、接触测绘数据¹¹。因此,VIE架构的适用具有高度局限性(且不排除未来自然资源部出台针对VIE架构的后续监管措施),纯粹外资背景的外国投资者很难通过VIE架构突破相关准入限制。

SECTION 003

结语

近年来,越来越多的境外投资者被中国高精地图市场蕴含的巨大潜力吸引,渴望能跻身其中、抢占先机。得益于国内日渐开放的市场环境以及各方对于合作架构、细节的谨慎考量,已经有部分外资通过各种途径率先布局中国市场,外资企业在境内高精地图行业的参与规模也相应呈现提升态势。但必须注意的是,出于高精地图行业特有的敏感性,外国投资者能够参与的业务范围和程序相当受限。2019年7月新修订的《外国的组织或者个人来华测绘管理暂行办法》仍保留了外资不得从事导航电子地图编制业务的原则,此举也体现了我国将持续对外资进入高精地图领域保持严格监管的监管思路。但是,另一方面,据了解,为借力境外先进技术、更好更快地发展我国高精地图,实践中业内人士对于适度允许外资参与导航电子地图领域的呼声渐高,不排除未来修订的《测绘资质管理办法》有对高精地图编制等外资禁区进行有限度放松的可能性。

即使如此,在可见的未来,外资想要参与中国高精地图行业,仍需结合自身需求,在对境内法规政策走向保持密切关注的同时,选择合适的架构(例如与有资质的境内合作伙伴开展一定合作),并在敲定合作架构、内容时重点关注业务范围,避免触碰政策红线。而对于拥有导航电子地图资质的境内公司来说,引入外资企业虽然有利于技术提升,但由于架构设计上的细微疏漏将可能危及资质、甚至存在行政乃至刑事责任风险,境内公司在选择合作方及合作模式上,势必需要慎之又慎,针对每一个合作步骤仔细考量,以实现获得收益和规避风险的共赢。

PART III

数据安全保护

12. 参见《关于加强自动驾驶地图生产测试与应用管理的通知》

13. 根据《测绘管理工作国家秘密目录》，从1:50万到1:1万的我国常用国家基本比例尺地形图及数字化成果均属于国家秘密的范围。

14. 参见《中华人民共和国保守国家秘密法》

在信息时代，“数据就是新的石油”。对于高精地图而言，石油不重要，数据却是不可或缺的部分。我国关于高精地图领域的法律法规尚不全面，高精地图数据的保密处理和公开使用等方面的政策仍在研究制定中¹²。现阶段高精地图的数据安全问题主要受制于与导航电子地图和互联网地图相关的法律法规。

SECTION 001

国家安全的保护

高精地图需要协助自动驾驶车辆实现准确定位、环境感知和路线规划等基础功能，因此需要测绘、采集大量的数据作为地图制作的基础。鉴于高精地图涉及国家秘密¹³等国家安全的问题，高精地图数据受到国家的严格控制，按照涉密测绘成果进行管理。高精地图数据的保密要求贯穿于地图制作的各个环节，接触高精地图数据的所有主体都受制于国家对于涉密信息的要求，任何人不得非法复制、记录、存储相关数据和信息。如有违反，则会被依法给予处分，甚至可能被追究刑事责任¹⁴。除了一般性的保密要求外，在高精地图制作的不同阶段，国家也通过不同的法律法规提出了相应的特别要求。

1. 数据采集

高精地图制作的第一步是进行测绘和数据采集，也是高精地图制作的基础。根据《中华人民共和国测绘法》，测绘是指对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述，以及对获取的数据、信息、成果进行处理和提供的活动；测绘活动的开展应以拥有测绘资质证为前提。

由于高精地图的数据主要利用车辆配备专业设备进行采集，核心采集设备包括摄像头和/或激光雷达。对于仅使用摄像头采集而言，如果只限于用图片记录周边环境，达不到对地理要素和人工设施的“形状、大小、空间位置”进行“测定、采集、表述”的程度，一般不会被认定为是测绘活动。由于激光雷达设备具有高精度测量、能够准确反映目标信息的特点，在实践中受到高精地图制作方的广泛青睐和使用。利用激光雷达等设备进行数据收集的活动，通常达到测绘的标准，会被认定为属于“测

15. 国家测绘地理信息局前身为国家测绘局,于2018年3月合并到自然资源部。

16. 参见《自动驾驶地图测试与管理通知》

17. 同上



绘活动”的范畴,数据收集的主体应具备相应的测绘资质。

高精地图主要将服务于自动驾驶系统,高精地图制作方在制作高精地图的过程中可能会与汽车企业等相关方合作开展地图的研发测试活动。而如我们在第一部分所述,高精地图的数据采集等测绘活动须由具有导航电子地图资质的单位进行。因此,合作各方需要注意,根据国家测绘地理信息局¹⁵的规定,在研发测试活动中所涉及到的测绘活动,必须由拥有导航电子地图资质的高精地图制作方单独从事,汽车企业等合作方不能直接参与测绘和数据采集环节¹⁶。

数据采集方在采集高精地图的数据时应严格遵守《导航电子地图安全处理技术基本要求》的相关限制性要求,谨慎防止采用各种测量手段获得限制采集的特定地理空间的信息,包括:重力数据、测量控制点;高程点、等高线及数字高程模型;高压电线、通讯线及管道等,避免带来国家安全相关问题。

2. 数据储存

国家要求高精地图数据按照涉密测绘成果进行管理¹⁷。依照《测绘资质管理规定》和《测绘资质分级标准》的规定,拥有导航电子地图资质的测绘单位在储存地图数据时应当采取必要手段保证相关数据的安全,如:配备必要的保密设备和设施;涉密设备和网络必须与互联网物理隔离;数据生产环节中的数据必须使用经加密处理的自有格式等。此外,对于互联网地图服务商而言,既需要确保在制作的地图中过滤、删除国家有关规定关于在地图上不得表示的内容,其用于提供服务的地图数据库

及其他数据库也不得存储或记录相关的信息¹⁸。

3. 数据传输

高精地图制作方不得随意向他人传输或提供其所形成的测绘成果。在数据传输中,又尤以数据出境问题最为受到国家安全层面的关注,国家特别制定了一系列相应法律法规进行规范。

(1) 一般规定

涉密信息系统严禁接入互联网及其他公共信息网络等未采取保密措施的数据传输网络中。在高精地图制作过程中能够接触到相关数据的主体都应当避免在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递相关数据,或者将涉密计算机、涉密存储设备接入互联网及其他公共信息网络等行为¹⁹。此外,根据《关于加强自动驾驶地图生产测试与应用管理的通知》(“《自动驾驶地图测试与管理通知》”)的规定,未经依法审批,地图制作方将不得向外国的组织和个人以及在我国注册的外商独资和中外合资、合作企业提供涉密测绘成果资料,也不得允许无关人员接触地图数据。

(2) 数据出境

a. 前置程序限制

数据出境需要完成相应的审批程序方可施为。正如前文所述,地图制作方若欲向外国的组织和个人提供涉密测绘成果资料,需要经过主管部门的批准。

《中华人民共和国网络安全法》(“《网络安全法》”)对数据出境提出安全评估的要求,关键信息基础设施²⁰运营者在境内运营中收集和产生的个人信息和重要数据应当储存在境内;如果因为业务需要必须向境外提供的,应按照国家网信部门等监管机构制定的办法进行安全评估。国家互联网信息办公室(“网信办”)发布的《个人信息和重要数据出境安全评估办法(征求意见稿)》(“《评估办法意见稿》”)中,将数据出境的评估要求从关键信息基础设施运营者,扩大到全部网络运营者,也即全体网络的所有者、管理者和网络服务提供者²¹。如若该征求意见稿最终按照其现有规定的内容生效,即使高精地图制作方未被认定为是“关键信息基础设施”的运营者,也需要在数据出境时进行安全评估²²。

b. 安全评估要求

关于安全评估的具体规范和操作指南仍在制定中,包括《评估办法意见稿》和《信息安全技术 数据出境安全评估指南(征求意见稿)》(“《评估指南意见稿》”)这两部还未生效的规范。《评估指南意见稿》中以定义和

18. 参见《地图管理条例》。

19. 参见《中华人民共和国保守国家秘密法》、《关于加强涉密测绘地理信息安全管理的通知》。

20. 根据《网络安全法》,关键信息基础设施是指:涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域,以及其他一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的相关信息基础设施。

21. 参见《评估办法意见稿》。

22. 根据《评估指南意见稿》,数据出境安全评估着重考察数据出境的必要性、涉及个人信息及重要数据的情况、数据出境对于国家安全、社会公共利益和个人合法利益的风险等方面。

23.《网络安全法》未对“数据出境”进行定义；《评估办法意见稿》中“数据出境”，是指网络运营者将在中华人民共和国境内运营中收集和产生的个人信息和重要数据，提供给位于境外的机构、组织、个人。

24.根据《导航电子地图安全处理技术基本要求》，不得在导航电子地图上出现的内容包括：与军事相关的单位和设施、与公共安全相关的单位和设施等重要信息。

25.参见《关于导航电子地图管理有关规定的通知》

26.参见《关于进一步加强地图导航定位产品统一监管工作的通知》

27.参见《关于导航电子地图管理有关规定的通知》

列举两种方式对“数据出境”进行界定，可能在一定程度上为各方参考而扩大“出境”的含义范围²³。根据《评估指南意见稿》，数据出境，是指网络运营者通过网络等方式将数据提供给境外的机构、组织或个人的活动。构成数据出境的情形包括：

(1) 向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据；

(2) 数据未转移存储至本国以外的地方，但被境外的机构、组织、个人访问查看的（公开信息、网页访问除外）；和

(3) 网络运营者集团内部数据由境内转移至境外，涉及其在境内运营中收集和产生的个人信息和重要数据的。

根据《评估办法意见稿》，个人信息和重要数据的出境需要互联网运营者根据评估要求自行测评，并报经行业主管部门同意。但如果出境数据体量或者性质达到一定标准，诸如数据量超过1000GB、包含敏感地理信息数据等重要数据的，按照《评估指南意见稿》的规定，就需要经过行业主管部门或监管部门的评估，并上报到国家网信部门。如果通过评估之后，出境的数据、数据接收方等重要相关信息发生重大变化，即需要重新进行安全评估。此外，对于出境会影响国家安全、社会公共利益以及经主管部门认定不得出境的数据，将不被允许出境。

4. 数据发布

在地图制作方采集到所需要的信息并进行数据整理之后生成的高精度地图不能直接发布。高精地图在公开出版、展示和使用之前还需要履行安全处理程序：涉及国家秘密和其他不得表达的属性内容不能够以任何形式表达在地图中²⁴，地图制作方需要对该等内容进行过滤并删除。除此之外，高精地图还需要经过国家测绘局指定的机构进行空间位置的保密技术处理²⁵。

经过技术处理的高精度地图需按照规定程序送至国家测绘局审核并取得审图号后，方可进行公开出版、展示、登载和销售；如有违反，地图制作方会受到相应的行政处罚²⁶。值得注意的是，即使初次制作的地图经过审核得以发布，地图制作方每一次改变地图内容（包括地图数据格式转换、地图覆盖范围变化、地图表示内容更新等），都需要按照规定程序重新送审²⁷。

国家测绘局对于互联网地图的审查程序相较于对于传统的导航电子地图而言，采用了更加灵活的方式——离线和在线审查相结合。高精地图制作方在构建好互联网地图服务运行系统（平台）后，向审查部门提供基

于互联网的内部网址和登录账号,即可通过在线审查完成地图公开前的审核步骤²⁸。

28. 参见《关于加强互联网地图管理工作的通知》

29. 参见《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》

SECTION 002

个人信息保护

为保证自动驾驶的安全,高精地图的不仅需要为自动驾驶系统提供精确的道路及周边环境的物理特征,也需要反映其他交通参与主体的信息,包括该等主体的位置、速度、行驶方向、路线等。高精地图所依附的车载导航系统需要对于汽车的实时状态及历史路径等信息进行持续记录,并通过车联网,使自动驾驶汽车彼此之间进行实时信息交互。高精地图和车联网的结合,在助力自动驾驶技术发展的同时,也增加了用户个人信息泄露的风险(如通过大数据计算可以轻易得出用户的出行习惯、常去地点等)。

我国对用户个人数据的安全性保护要求贯穿于互联网地图服务提供者所实施的从用户个人信息收集、使用到存储及出境等各个环节,地图服务方应当在各个环节均采取必要方式确保减少用户个人信息所面临的安全性风险。

按照《网络安全法》的规定,网络运营者不得收集与其提供的服务无关的个人信息。互联网地图服务方收集数据时应遵循最少够用原则,收集满足业务所必须的最少类型和数量的信息。对于地图导航业务来说,参考全国信息安全标准化技术委员会制定的指南,地图导航功能所需要用户的必要信息应仅为用户的位置信息,包括精准定位信息和行踪轨迹。其中,精准定位信息仅应使用于确定用户位置,进行地图搜索和展示导航服务;而行踪轨迹仅应被用于实现导航服务中判断实施路况、重新规划导航线路的功能²⁹。

互联网地图服务方在收集用户的个人信息时,应该确保用户的知情权,征得用户的明示许可,且应当说明收集、使用信息的目的、方式和范围,秉承公开收集、使用规则。在使用用户地理位置等信息时,服务方应当进行适当的脱敏处理,避免在数据中出现可识别性的用户个人信息。对于收集到的用户信息,服务方也应当妥善保存该等信息数据,采取有效的技术措施和其他必要措施,防止用户的个人信息泄露、丢失,保障用户个人信息的安全。

互联网地图服务方须确保不泄露、篡改、出售或者非法向他人提供用户的个人信息,在用户个人信息因业务要求而需要出境时,也需要经过



安全评估方可进行。如果发现个人信息出境未经个人同意或者可能侵害个人利益的,该等信息的出境将被禁止。

SECTION 003

小结

高精地图的发展需要遵守国家有关数据安全和个人信息保护的要求,而数据安全和个人信息保护的要求亦有利于高精地图产业的良性发展。法律规范和科技发展从来都不是矛盾的存在。科技的发展会推动法律的进步和完善;相应地,法律的红线也将促使科技在可控范围内升级突破。因此,我们可以期待,在自动驾驶汽车缓缓向我们驶来的道路上,高精地图的发展和数据安全的保护也将寻找到一个合理的平衡点,共同助力中国自动驾驶的早日实现。

PART IV

众包模式

随着软硬件技术发展和应用场景演进,高精地图产业在数据采集、加工、存储、发布表达、更新及应用环节都发生着革命性的变化。在采集环节,从肉眼加测绘设备获取数据演变为通过各种采集终端、设备、传感器系统来获取数据,从基础测绘和遥感技术发展为社会化、大众化采集;在加工环节,从人工处理升级到人工智能多元自动化处理;在数据存储、发布表达及更新环节,从纸质载体发展为多媒体载体、从二维提升到三维、从静态发展到实时动态、从图纸记录升级到本地数据库及云端。在应用环节,除了日常导航、自动驾驶决策规划,高精地图也开始扩展到智慧城市等其他应用。在上述大背景下,“众包”作为新型的高精地图数据采集模式应运而生。在第四部分,笔者拟对众包模式的概念、现状以及存在的法律问题等方面进行讨论,供读者参考。

SECTION 001

众包模式的概念及现状

目前,高精地图数据采集主要分为集中制图和众包制图两种模式:

(1)集中制图模式:专门从事高精地图制备工作的有关实体(即本文提及之“图商”,在我国为具备导航电子地图甲级测绘资质(“导航电子地图资质”)的有关测绘单位)通过其自有专用数据采集车、以半自动化和全自动化的方式采集数据。集中制图模式获得的矢量地图精度高、可信度高,但采集成本也很高——单台自动驾驶级别高精度采集车的成本就近千万元人民币;同时“图商”还需常年维持规模在千人左右的数据采集团队,并在后台统一对采集的数据进行标注及补缺。目前,仅有少量资金雄厚的“图商”(如高德地图、四维图新、TomTom等国内外老牌图商)采用这种方式制图。

(2)众包制图模式:“图商”和/或其他数据采集商(“发包方”)利用配备激光雷达或摄像头等传感器技术的第三方普通车辆(如整车厂的量产车)进行实时数据采集,并上传到发包方的云服务器。这一模式又细分为以下两种数据采集方式:①视觉方式,即发包方通过在合作车辆上安装智能摄像头(如以色列的Mobileye)、智能后视镜、行车记录仪等或在合作司机用户手机上安装相关APP(如美国的Ivl5)的方式采集并上传数据;②雷达方式,即发包方(如美国的DeepMap)通过车载激光雷达获取

激光点云数据、轨迹和照片,利用人工智能识别处理地面路线、道路特征相关信息,实现地图更新。

相比集中制图模式,众包模式下收集的数据精度较低,但数据量大、采集成本低,并可获取大量实时动态信息(如道路拥堵、交通事故、天气情况等),实现分钟级甚至秒级的更新。同时,众包模式是典型的UGC(User Generated Content,即用户生成内容),通过大量行驶在路上的车辆采集数据,使用者同时也是数据的提供者——“取之于车,用之于车”。随着大数据技术的发展以及人工智能技术的突破,通过众包模式制备的地图的精度也在不断提升。此外,即便是依然采用集中制图模式的图商,也往往在制图过程中同时采用众包模式。例如,百度、HERE、TomTom等先以专业测绘采集车创建基本地图和语义层,随后采用众包模式使基础地图不断迭代,以达到实时更新的效果。行业内普遍认为,众包模式代表着高精地图产业的未来。

众包模式带来两项重要商业变化:一,大大节省制图成本、降低入门槛。例如,国内高精地图新锐极奥科技一开始就选择时间、资金成本较小的数据众包模式,不依赖价格高昂的专业测绘设备,从而降低成本;美国的lvl5将目标锁定在Uber等平台的司机用户上,就所获取的数据支付小额费用;而国内的滴滴、顺丰、京东也在利用车队优势抢滩高精地图。二,沉淀大量数据、扩大后续增值服务空间。过去,图商的商业模式主要是卖license(授权)给车厂;如今,更多图商在向空间位置大数据服务商转变,通过众包实现自动采集、智能处理分发模式,为自动驾驶车辆提供全方位的地理信息服务。不少传统图商及新锐都在和车厂进行一系列合作,由车厂在其销售的车辆上安装摄像头收集图像等信息,再由图商利用其平台将图像等信息转换成可实时更新的高精地图数据,随后向车厂等提供最终的高精地图应用产品和高精地图数据服务(包括众包数据更新、高精定位等)。

SECTION 002

众包模式面临的法律问题

通过不断的技术迭代和商业模式的演进,众包模式正在建立一个全新的地图数据采集、制图和更新的生态环境。另一方面,这一新兴的数据采集模式在现有法律制度下也面临着一系列的法律问题。具体如下:

1. 测绘资质问题

我国对从事测绘活动的单位实行测绘资质管理制度，高精地图的数据采集、编辑加工和生产制作必须由具有导航电子地图制作测绘资质的单位承担。那么，众包车主采集数据是否属于高精地图数据采集行为，进而需要取得导航电子地图制作测绘资质呢？

要回答这个问题，我们需要先找到以下问题的答案：

首先，众包车主在收集哪些数据？

一般来说，众包数据包括轨迹数据（融合定位形成高精度轨迹）、视频数据（通过标定和AI算法把图像数据变成矢量化数据）、雷达数据（精准测量、提升精度）以及车内传感器数据（车内各个零部件在毫秒级层面上输出的数据）。虽然部分企业（如极奥科技）会采用众包模式收集高精地图基础静态数据，大部分众包车辆更多是在收集动态交通对象（如行人、其他车辆或标牌系统）行为的丰富信息及动态变化的交通要素，如交通拥堵、施工点、交通事故等，即对应高精地图的动态地图数据部分。

其次，众包车主收集数据是否属于《中华人民共和国测绘法》（“《测绘法》”）下的“测绘行为”？

根据《测绘法》，“测绘是指对自然地理要素或者地表人工设施的形状、大小、空间位置及其属性等进行测定、采集、表述，以及对获取的数据、信息、成果进行处理和提供的活动”，即根据观测到的数据将地面的自然形态及人工设计绘制成地图。众包模式是在任何地点、任何时间，为认知周围环境和人/车而使用、收集及不断更新有关信息/数据的活动，即使众包车辆只收集动态信息，如路况、交通标志、障碍物、坑洼、建筑物、道路维修信息、交通事故等，也很可能被认定为属于对“地表人工设施的形状、大小、空间位置及其属性”的“测定、采集”。如果在众包模式下收集数据的类别和/或详细精准程度达到与测绘活动相同或相近的数据要求，则该等活动非常有可能被归入“测绘行为”范围。

此外，根据《关于导航电子地图管理有关规定的通知》，“除依法取得导航电子地图测绘资质的外，其他单位和个人在使用导航电子地图过程中，不得携带其他带有空间定位系统（如GPS等）信号接收、定位功能的仪器开展显示、记录、存储、标注空间坐标、高程、地物属性信息，以及检测、校核、更改导航电子地图相关内容等测绘活动”。如果数据采集仅使用雷达（不包括激光雷达等带有GPS系统的雷达）和/或摄像头，该等活动被视作测绘的可能性不高。但是，如果使用GPS、惯性导航装置或类似定位装置和/或激光雷达（集激光、全球定位系统和惯性导航系统三种技术于一身）采集数据，则很可能被认定为测绘活动。在上文提及的两种主要

数据采集方式(视觉方式和雷达方式)中,视觉方式主要利用相机并结合GPS(例如行车记录仪),雷达方式主要依赖激光雷达,均可能会涉及GPS等定位装置,其采集的信息极可能带有位置信息,因此该等活动很有可能被视作测绘活动。

如严格依照《测绘法》等法规,众包车主(例如有关个人车主)似乎很可能被认为在从事测绘活动,进而需取得有关测绘资质。但是,让诸多众包车主申请和维持有关测绘资质显然不现实。或许正因如此,对于众包模式收集数据是否构成测绘、有关主体是否需取得测绘资质,业界一直莫衷一是,而监管机构似也一直未明确其态度。

在众包模式下,不论众包车主采集的数据为何,其均将通过网络把数据上传到发包方的相应网络平台,由发包方进行存储、处理并相应整合到高精地图的数据包中。因此,如能对发包方就数据收集(例如,对于数据收集的硬件和软件标准提出要求)、上传、存储、处理和使用等形成完善的行业标准和监管制度,在一定程度上也可实现对众包模式的有效监管——正如目前对于短视频等其他UGC模式的商业模式监管。具体而言,除导航电子地图资质准入管理外,主管部门可考虑对平台运营方/发包方实施众包模式审查制度(与导航电子地图资质相结合),在技术上要求对众包采集的地理信息进行技术加密和保密传送等,并结合实时审核、定期报备及各项技术要求,对发包方和众包车主予以监管。

2. 数据合规问题

(1) 涉密数据保护

根据《关于加强自动驾驶地图生产测试与应用管理的通知》,用于自动驾驶技术试验、道路测试的地图数据(包括在传统导航电子地图基础上增添内容、要素或精度提升的),应当按照涉密测绘成果进行管理;未经省级以上测绘地理信息行政主管部门批准,不得允许超出范围的人员接触地图数据。众包模式下,存在大量外部人士(例如,众包车主、采集软件/设备所有方、车厂、云端数据控制者及接触者等)采集或接触涉密数据,似乎难以满足前述规定。另外,众包模式下数据的传输、储存等均通过云端,亦难以满足有关法律规定的地图数据传输和储存要求。因此,众包模式下的数据实践与数据安全法律规定存在较大矛盾。

就此,一方面,发包方应对相关地图数据进行技术加密,同时建立保密传送及限制未经授权的第三方访问云端数据库等机制,使外部人士无法实质性地接触数据或获取数据。另一方面,虽然加强数据安全保护是大势所趋,但相关数据立法也需随着技术和商业环境的演进发展与时俱

进,在发展与安全中寻得平衡。正如《测绘法》所明确的,测绘成果的秘密范围和秘密等级,应当依照保密法律、行政法规的规定,按照保障国家秘密安全、促进地理信息共享和应用的原则确定并及时调整、公布。

(2) 个人数据保护

除上述地图数据外,众包模式下的数据采集还涉及个人数据保护问题。在数据集中获得的行人、其他各类车辆驾驶人员和/或自行车骑车人的面部影像或背景图像、出行信息以及其他活动/行为数据,均属于个人数据的范畴。根据我国《网络安全法》和《儿童个人信息网络保护规定》等规定,采集与使用个人信息须遵循知情同意原则。显然,在众包模式下采集数据前取得每个主体的同意并不现实。目前,发包方通常遵循采集和处理行人及其他相关个人影像方面的有关惯例。例如,在设计采集设备时尽可能减少自动驾驶汽车产生、收集或保留的个人信息量或配备人脸模糊化软件,以使得相关影像中无法识别出个人、对收集到的信息采取加密和匿名化、并且建立防止滥用或未经授权的第三方访问等机制。

需要指出的是,我国正在不断加强个人信息保护立法。《个人信息保护法》和《数据安全法》已列入2020年立法工作安排,《数据安全管理办法(征求意见稿)》等规范性文件与《信息安全技术 个人信息去标识化指南(征求意见稿)》、《信息安全技术个人信息安全影响评估指南(征求意见稿)》、《信息安全技术个人信息安全规范(2020正式稿)》等国家标准都陆续出台。众包模式的参与方也需根据法律法规的变化及时更新其技术和商业模式。

(3) 数据所有权

众包模式下,数据采集设备供应商往往通过其设备/系统与车厂、车主合作采集数据,并由图商对数据进行加工/清洗等工作。如上文所述,高精地图测绘活动仅得由具备相关资质的主体开展,有关测绘数据只能由有资质的主体掌握(也即相应排除其他方拥有该等数据的可能性)。同时,如果涉及个人数据,其所有权通常也应归于个人所有。对于众包模式下采集获得的其他数据,诸如动态数据的所有权归属等,在法律方面尚无定论。因此,众包模式的参与各方可考虑在相关合作协议中明确有关数据的归属、许可使用安排等相关事宜,以增强这一模式的合规性。

SECTION 003

展望

众包模式具有其特有的优势,主要体现在成本低、收集数据范围广、实现实时更新等方面,而随着技术的发展,其精度低的欠缺也会逐渐被攻克。从法律角度来看,自动驾驶的蓬勃发展,在生产力层面提出了众包模式的现实需求,必然要求相关法规政策因时而变、顺势利导,方能更好地适应自动驾驶的需要。如果在法律制度和监管手段上能够对众包模式进行创新性和与时俱进的改革,将有助于我国在全球自动驾驶及智慧城市领域争得领先地位。同时,我们也期待有关企业把握大势、抢抓机遇,成为自动驾驶时代的中流砥柱,共同绘制众包模式及自动驾驶的美好未来。

附件 导航电子地图资质企事业单位一览表

企业名称	获得资质时间	公司背景	股东所属行业/类型
北京灵图软件技术有限公司	2005.05	图商	科技公司 (电商/IT)
立得空间信息技术股份有限公司	2007.06		
武汉光庭信息技术股份有限公司	2013.06		
江苏智途科技股份有限公司	2019.05		
北京四维图新科技股份有限公司	2001.01	图商——2014年腾讯11.7亿元收购四维图新11.28%股权	
深圳市凯立德科技股份有限公司	2005.06	图商——2014年小米全资子公司8400万元入股	
易图通科技(北京)有限公司	2005.07	图商——2010年阿里巴巴集团收购其60%股权	
高德软件有限公司	2004.06	阿里巴巴子公司——2014年被阿里巴巴集团全资收购	
北京长地万方科技有限公司	2005.05	百度子公司——2013年被百度全资收购	
腾讯大地通途(北京)科技有限公司 ³⁰	2007.06	腾讯子公司——2014年被腾讯全资收购	
北京华为数字技术有限公司	2019.07	华为子公司	

30.曾用名:科菱航睿空间信息技术有限公司。

北京京东叁佰陆拾度电子商务有限公司	2020.01	京东子公司	
丰图科技(深圳)有限公司	2019.11	顺丰子公司	物流
滴图(北京)科技有限公司	2017.10	滴滴子公司	交通出行
武汉中海庭数据技术有限公司	2018.08	上汽子公司	车企
北京初速度科技有限公司(Momenta)	2018.08	自动驾驶算法公司	自动驾驶
贵州宽翼智云科技有限公司	2019.01	自动驾驶公司	
江苏晶众信息科技有限公司	2019.05	自动驾驶公司	
国家基础地理信息中心	2006.01	事业单位	
江苏省测绘工程院	2008.06		
浙江省第一测绘院	2008.06		
江苏省基础地理信息中心	2010.10		



邱建/合伙人
资本市场部
北京办公室
+86 10 5957 2092
qujian@zhonglun.com



朱永春/合伙人
公司二部
北京办公室
+86 10 5957 2488
zhu Yongchun@zhonglun.com



陶媛园/非权益合伙人
资本市场部
北京办公室
+86 10 5957 2165
taoyuanyuan@zhonglun.com



4

CHAPTER 02

数字金融的应用、 监管及合规思考

作者:樊晓娟/印磊/洪嘉宾/竺雨辰

以人工智能、云计算、区块链等为代表的基于新一代信息技术演化生成的信息基础设施被国家发改委明确列入新型基础设施范围,而这些基于新一代信息技术基础设施的金融科技创新催生了数字金融,成为金融领域的新业态和新模式。数字金融及其所依赖的金融科技已经聚焦了来自全球的监管机构、金融行业和科技领域的目光。

在中国内地,中国人民银行于2019年8月发布《金融科技(FinTech)发展规划(2019-2021年)》强调金融科技成为推动金融转型升级的新引擎,提出金融科技的六大发展目标¹;在中国香港,香港交易所结算有限公司于2018年10月18日研究报告《金融科技的运用和监管框架》,着重围绕区块链和人工智能这两大技术与证券行业的结合点展开,说明金融科技对资本市场和证券交易的影响和意义;在新加坡,新加坡金融监管局(MAS)近五年来,每年都会组织SFF x SWITCH²,回顾、展望和探讨金融科技的发展;在瑞士,联邦议会(Federal Council)于2018年12月7日发布Legal framework for distributed ledger technology and blockchain in Switzerland An overview with a focus on the financial sector(《金融角度概览:瑞士关于分布式记账技术及区块链的法律框架》)关注和探讨了以分布式记账作为基础技术在金融领域的应用。

1. 金融科技应用先进可控、金融服务能力稳步增强、金融风控水平明显提高、金融监管效能持续提升、金融科技支撑不断完善和金融科技产业繁荣发展。
2. The Singapore FinTech Festival (SFF) and the Singapore Week of Innovation and Technology (SWITCH), 简称SFF x SWITCH。

3.全球金融稳定委员会对金融科技(FinTech)的定义, <https://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/>

SECTION 001

数字金融的基本理解

人们对于数字金融一词已经耳熟能详,但是又应当如何理解数字金融呢?

(一) 依赖新型信息基础设施

金融科技指金融服务领域的科技创新,这些科技创新形成对金融市场和金融服务供给产生重大影响的新业务模式、新技术应用和新产品服务就是金融科技(FinTech)³。前述对于金融科技的定义由全球金融稳定委员会(Financial Stability Board,“FSB”)提出,被全球普遍认可。

数字金融是金融科技的产物,所以,其研发和应用必然依赖于人工智能、云计算、区块链等新型信息基础设施。

(二) 应用范围广泛

不同于金融科技,数字金融并没有被普遍接受的定义。因此,我们只能从数字金融的应用现状来框定数字金融的范围。综合全球监管机关的各类官方出版物(包括但不限于指引、研究报告、白皮书)对于数字金融的探讨,我们理解,数字金融的应用范围至少包括以下类别:

1. 供应链金融

供应链金融,顾名思义,是一种银行向核心企业提供融资和其他结算、理财服务,同时向这些客户的供应商提供贷款及时收达的便利,或者向其分销商提供预付款代付及存货融资服务,是由核心企业与银行间达成的,一种面向供应链所有成员企业的系统性融资安排。

例如腾讯云融资易的动产质押融资平台,通过物联网、大数据、人工智能技术联动,对进场货物进行识别、采集、监控或告警,并将相关事件记录在区块链上,实现仓单记载货物信息的真实可信。同时仓单也可转化为链上数字资产,实现质押交易流程数字化管理,一定程度上规避了货物重复融资的风险。

2. 贸易融资

贸易融资,是指银行运用结构性短期融资工具,基于商品交易中的存货、预付款、应收账款等资产的融资。

区块链贸易融资平台可以有效提高交易效率及准确性,提高融资透明度,降低融资风险,为贸易融资提供全新的解决方案。香港金管局、汇丰银行、中国银行、东亚银行、恒生银行和渣打银行及德勤就联合建立了

区块链贸易融资平台“贸易联动(eTradeConnect)”。

3. 智能投顾业务

投顾业务,也就是资产投资顾问服务,服务提供者通过数据分析、模型搭建等方式提供资产配置建议。而智能投顾则是运用人工智能技术基于资产组合理论相关算法来搭建数据模型和后台算法,为投资者提供智能化和自动化的资产配置建议。

例如广发证券于2016年推出的智能投顾品牌“贝塔牛”,正是通过人工智能“选股+择时”,并结合大数据分析,根据不同客户的投资目标及风险承受能力,给出不同的投资理财策略。

4. 互联网保险业务

保险业务,即保险公司经营的保险产品的承保、理赔等相关活动。在蚂蚁金服提供的“保险数据中台”、“保险上云”等服务中,借助大数据、云计算、人工智能等金融科技手段,为众安保险、中国太平等多家保险公司,提供了全系统上云,完善大数据产品,多维人工智能方案,实现从5秒处理1单到每秒处理1000单,使中国保险业务正式进入互联网保险业务新时代。

5. 数字银行业务

数字银行,或称虚拟银行,指传统银行业务依赖互联网平台,为大众提供全面数字化的存款、支付、借贷等银行服务。

香港金管局于2019年3月至5月颁发了8家虚拟银行牌照,其中不乏有腾讯、蚂蚁金服、平安、京东、小米、众安等中国金融科技巨头的身影。截止2020年4月底,众安银行已正式营业,另有4家虚拟银行已开始试营业。

6. 支付服务

支付服务,一般是由服务提供商作为收付款人之间的中介人提供支付、收单等业务服务。而互联网的快速发展,使得支付领域成为金融科技应用的高地。支付宝、微信等第三方支付巨头通过扫码、NFC等技术极大地推动了中国社会的无现金化进程。而随着央行数字货币的诞生,人工智能、区块链、开放API等技术的应用,将共同形成新一代支付生态体系,在原来互联网支付的基础上进一步增强支付智能化发展,减少对中介机构的依赖。而条码支付、刷脸支付等互联互通技术验证与应用试点,将推动KYC和交易验证手段升级,进一步加强支付风险防控。

(三) 积极意义

数字金融的应用落地和推广至少有以下积极意义。

4. 中国人民银行,《金融科技(FinTech)发展规划(2019-2021年)》,2019年8月

5. 中国人民银行,《金融科技(FinTech)发展规划(2019-2021年)》,2019年8月

6. Libra是由Facebook联合数十家互联网科技公司发起的全球稳定币项目,其旨在以区块链技术为基础,以多种法币等稳定资产储备为背书,成就一种在亿万人中自由流通的全球性货币。详见www.libra.org

1. 推进普惠金融

联合国于2005年首次提出了普惠金融(financial inclusion)的这个概念。普惠金融是指立足机会平等要求和商业可持续原则,以可负担的成本为有金融服务需求的社会各阶层个人或企业提供适当、有效的金融服务。普惠金融一直是政府需要推进的惠民政策之一。基于普惠金融面向大众而成本高、收益较低、安全和效率难以兼顾的特征,金融企业投入运行普惠金融产品的积极性大多不高。

大数据、人工智能及区块链等技术加持的数字金融应用可以有效降低普惠金融产品的运营成本,进一步扩大普惠金融的影响范围。

2. 优化金融服务能力

借助机器学习、数据挖掘、智能合约等技术,数字金融有助于简化供需双方交易环节,降低资金融通边际成本,开辟触达客户全新途径,推动金融机构在盈利模式、业务形态、资产负债、信贷关系、渠道拓展等方面持续优化⁴。

在此情况下,企业和个人作为数字金融产品的用户,其投融资成本和便利性也有望得到大幅优化。

3. 提高金融业务风险控制能力

数字金融可以运用大数据、人工智能等技术建立金融风控模型,有效甄别高风险交易,智能感知异常交易,实现风险早识别、早预警、早处置,提升金融风险技防能力。⁵

4. 促进全球经济一体化进程

数字金融基于新一代信息基础设施。金融科技的利用创新的快速、低成本、安全的数据传输和交互条件,从而为数字金融产品和服务跨境供给了极大便利。在可预计的未来,众多数字金融产品或服务会在全球范围运营。Libra白皮书描绘的金融体系就是一个典型的例子⁶。

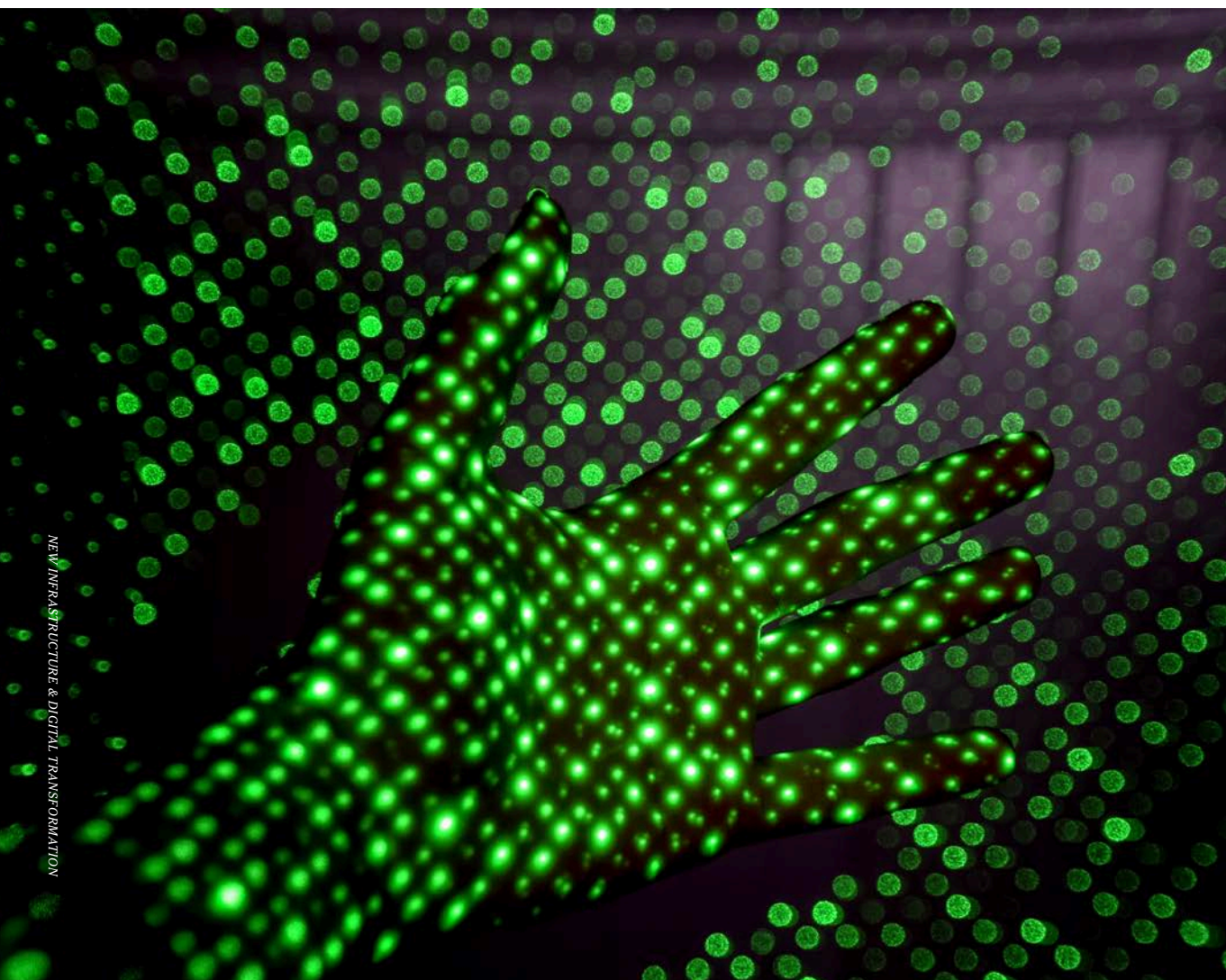
SECTION 002

数字金融的特别监管方法——金融监管沙盒

基于金融科技的数字金融是金融产品和服务的新业态、新模式。创新难免会伴随不可预测的风险。如何有效把控风险的同时又能为数字金融发展提供充分的空间?

英国金融行为监管局(UKFC)于2015年首次把计算机中的沙盒概念引入金融监管,创立了金融监管沙盒制度。监管沙盒的基本含义是,创新金融业务在监管机构的严格监管且有限制的环境下运营,以有效防控

未来中国央行数字货币DCEP落地,可能很大程度上改变人民币在与美元、欧元等全球流通货币竞争中的位势。



7.http://210.12.10
2.231/public/pub-
licity

风险,并在风险发生时及时暂停、改进相关创新业务。在此情况下,金融创新中的未知缺陷所可能造成的损失,可以得到有效控制,避免损失无限扩大。

目前,英国、新加坡、加拿大、印度以及中国香港等均已实行金融监管沙盒制度。在这些国家和地区,已经有相当一部分创新业务通过了沙盒试验,正式投入市场,对丰富金融产品、活跃金融市场产生了积极作用。

而中国版沙盒也已推出。2020年央行北京营管部公告了首批一共6个试点项目,已经开始向用户正式提供服务⁷。中国版沙盒将有效帮助金融科技将创新动力化为实践,促使数字金融产业落地和发展,紧跟国际金融市场的脚步,使我国金融科技得到长足发展。

SECTION 003

数字金融的合规考虑重点

结合数字金融依赖于金融科技的特点,我们认为数字金融产业至少有以下合规重点:

(一) 业务资质

数字金融产业参与者根据其参与程度的不同,可能会涉及金融、保险、证券、支付等业务,并受到相关法律法规的管理,需要获得国家有关部门行政许可后,方可参与经营活动。但是如果金融科技服务商仅向金融机构等提供技术服务支持的,则无需获得该等行政许可。

以在我国境内从事金融银行业务为例,根据《银行业监督管理办法》、《金融许可证管理办法》等规定,设立银行业金融机构或者从事银行业金融机构的业务活动应当取得国务院银行业监督管理机构批准。因此数字金融产业的参与者涉及数字银行业务的,应当在事先获得金融许可证。另外,特别针对区块链相关信息服务提供者,我国《区块链信息服务管理规定》规定,在我国境外提供区块链信息服务的,应在十个工作日内通过网信办区块链信息服务备案管理系统履行备案手续。

又例如,香港证监会发布的《证券及期货条例》把10类金融业务牌照列为受规管业务,应取得牌照方可经营。其中,7号牌就是针对提供证券、期货、外汇等线上交易服务商。4号牌、5号牌则是针对提供证券投资、期货投资意见的服务机构。

(二) 证券发行流通的审批

通证发行相关的数字金融业务,若被认为属于证券范围,可能会涉及证券发行流通方面的审批、监管。

例如,对于新兴技术带来的这个“通证”产品,美国证券交易委员会(the U.S. Securities and Exchange Commission, “SEC”)于2019年4月发布了《数字资产监管框架》⁸,建议参考“豪威测试”来界定企业融资时发行的通证是否属于证券型通证。若被认定为证券型通证,则该通证的公开发行人和交易则必须遵守包括《1933年证券法》和《1934年证券交易法》在内的各项证券法规的规定,必须向SEC进行注册或者豁免备案。

(三) 反洗钱、反恐融资

反洗钱、反恐怖融资一直都是传统金融行业的合规重点。而金融科技的应用,尤其是区块链等技术,因其匿名性的特征,极易被不法分子用作洗钱或恐怖主义融资的渠道,反洗钱、反恐融资更是监管工作的重中之重。各国以及反洗钱金融行动特别工作组(Financial Action Task Force on Money Laundering)都制定了关于反洗钱、反恐怖融资的法律规定。我国的反洗钱法对于银行⁹及特定金融机构¹⁰建立KYC制度、可疑交易报告制度等反洗钱义务也作出了规定。数字金融服务相关机构应当依据所适用的法律建立健全客户身份识别制度、客户身份资料和交易记录保存制度、大额交易和可疑交易报告制度,履行反洗钱、反恐融资义务;而数字金融技术服务商应积极配合金融机构利用金融科技建立KYC、交易监管等措施,以此来应对洗钱、恐怖融资等非法行为。

(四) 数据保护

金融科技技术服务商,无论是提供区块链平台、大数据、云计算服务,还是在KYC过程中,均会接触到大量个人信息数据。服务商应当根据我国《网络安全法》、《电信和互联网用户个人信息保护规定》等相关法律法规,建立完善的数据获取、利用、传输机制。

特别注意的是,数字金融服务中可能涉及大量个人金融信息¹¹。除符合一般性的数据保护规定外,相关服务方还应当遵守个人金融信息的特别规定,例如采取加密、去标识化、匿名化等技术手段、限制跨境传输等。

除我国相关规定外,金融科技服务技术商在境外提供技术服务,若涉及收集个人信息的,应当符合各国关于用户隐私数据保护的法律法规,例如:欧盟的通用数据保护条例(General Data Protection Regulation)、美国的美国联邦贸易委员会法(Federal Trade Commission

8. Framework for 'Investment Contract' Analysis of Digital Assets

9.《中华人民共和国反洗钱法》第三条规定:“在中华人民共和国境内设立的金融机构和按照规定应当履行反洗钱义务的特定非金融机构,应当依法采取预防、监控措施,建立健全客户身份识别制度、客户身份资料和交易记录保存制度、大额交易和可疑交易报告制度,履行反洗钱义务。”

10. 中国人民银行于2018年7月26日发布的《关于加强特定非金融机构反洗钱监管工作的通知》,应履行反洗钱义务的“特定非金融机构”包括房地产开发企业、贵金属交易所、会计师事务所、律师事务所、公证机构、公司服务提供商等。

11. “个人金融信息”是指金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息,包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

Act)及各州的相应法律。

(五) 外汇监管

Libra等基于区块链技术的全球稳定币在未来将为用户的跨境支付提供便利并且可以与法币实现双向兑换,打通不同法域之间法币流通的障碍,这必然会涉及到外汇问题。在实施外汇管制的法域,例如我国,Libra等稳定币的前述兑换功能很有可能被外汇监管部门认为是变相买卖外汇而受到调查和监管。

未来中国央行数字货币DCEP落地,可能很大程度上改变人民币在与美元、欧元等全球流通货币竞争中的位势,也为DCEP与Libra等全球稳定币的竞争中注入强劲动力。

(六) 税收

随着数字金融的不断发展,资产数字化交易的税务问题,也陆续产生。数字金融服务商除了遵守传统税务规定外,在提供服务中若收取或支付任何数字货币形式的对价,应当按照当地的税收规定依法纳税。

SECTION 004

结语

新型基础设施范围的明确,无疑展现了我国对于金融科技的认可。随着上述这些金融科技的不断发展,数字金融领域的应用及创新也将不断增多,并大范围落地。但对数字金融领域的参与者来说,随着法律法规的配套完善,以及应用具体实践,各类合规问题可能会不断涌现。作为法律人士,我们愿与各类金融科技企业一同成长,为各企业发展保驾护航,也为我国新基建的发展贡献自己的力量。



樊晓娟/合伙人
资本市场部
上海办公室
+86 21 6061 3669
fanxiaojuan@zhonglun.com

CHAPTER
THREE

DEVELOPMENT & IP PROTECTION

叁

开发 与知识产权保护篇

CHAPTER THREE





1

CHAPTER 03

人工智能生成物 能否获得法律保护？

作者:陈际红/钱璐

时至今日,全球产业界已经充分认识到人工智能技术引领新一轮产业变革的重大意义,世界主要发达国家均把发展人工智能技术作为国家重大战略。习近平总书记指出,加快发展新一代人工智能技术是事关我国能否抓住新一轮科技革命和产业变革机遇的战略问题。

人工智能技术已经能够“创作”出一些绘画、诗歌、乐曲等内容,比如微软小冰于2017年独立“创作”了诗集《阳光失了玻璃窗》,谷歌的Deep Dream可以将人类输入的图像转化为具有独特画风的图画,腾讯开发了能自动化撰写财经类新闻报道的Dreamwriter软件等。人工智能生成的内容(“人工智能生成物”)能否获得保护,构成了对现有法律制度的挑战。随着人工智能技术的进一步发展,问题可能会变得愈发复杂,人工智能生成物能否获得充分的法律保护关系到产业发展。

SECTION 001

人工智能的“创作”

当前的人工智能已经超越一般计算机程序,在“创作”过程中,不再是单纯被动地接受程序员指令,而是可以基于算法在一定程度上自主学习、计算和输出。在此技术背景下,我们可以将人工智能生成物理解为由计算机根据环境和算法独立生成的内容。

一般而言,人工智能“创作”过程中涉及到如下各方利益:(1)人工智能程序开发者(如:开发微软小冰的微软公司);(2)人工智能程序应用者(其从开发者获得授权,将人工智能程序应用于各种场景);(3)人工智能程序训练过程中所使用的既有作品的权利人。人工智能程序的“创作”能力并非凭空而生,人工智能程序需要对大量数据(包括受著作权法保护的作品)进行学习和分析,以形成自己的“创作”素材或规则,有的“创作”会直接在既有作品上进行演绎(如:谷歌的Deep Dream)。

如今,人工智能商业化应用愈发普遍,讨论人工智能生成物的保护,以及各方对其拥有的权益具有现实意义。

SECTION 002

人工智能生成物获得著作权法保护的条件

人工智能生成物构成著作权法意义上的作品是其获得著作权法保护的前提。

根据《中华人民共和国著作权法实施条例》第二条,著作权法所称作品,是指文学、艺术和科学领域内具有独创性并能以某种有形形式复制的智力成果。据此,作品的构成要件可归纳为:(1)具有独创性;(2)具有可复制性;和(3)属于文学、艺术和科学领域的内容。一般情况下,作为计算机程序的直接产物,人工智能生成物可以满足要件(2)和要件(3),具有争议的是其是否满足要件(1)。

(一) 独创性考虑

是否具有独创性是判定人工智能生成物是否构成作品的重要考量因素。归根结底,著作权法根本的立法目的是激励人类的智力型活动,以创作出更多有益于社会的作品,而非单纯对社会投资或劳力付出回报。就此问题的厘清,美国最高法院于1991年对费斯特一案(Feist Publications, Inc. v. Rural Telephone Service Company)的判决具有里程碑

的意义。这一判决排除了“额头出汗”和“辛勤收集”原则在确定著作权法保护范围时的适用,同时,法院据此认为,因电话号码簿没有足够的独创性,而仅是经辛苦努力后编写出的资料,故其不能受到著作权法的保护。

我国著作权法虽然在作品定义中阐述了独创性,但并未明确规定独创性的具体内涵和法律判定标准。尽管如此,有关司法解释及法院的审判指南中对“独创性”的内涵进行了一定的解读。如:《最高人民法院关于审理著作权民事纠纷案件适用法律若干问题的解释》第十五条规定:由不同作者就同一题材创作的作品,作品的表达系独立完成并且有创作性的,应当认定作者各自享有独立著作权。北京高级人民法院发布的《侵害著作权案件审理指南》第2.2条规定了认定独创性时应当考虑的因素:(1)是否由作者独立创作完成;(2)对表达的安排是否体现了作者的选择、判断,及认定表达是否具备独创性与其价值无关。需注意,即便司法实践中对独创性的认定形成了一定的原则性判定标准,在判定一个创作物是否具有独创性时,还应当依据个案的具体事实进行具体分析与判断。就人工智能生成物是否具有独创性这一问题,笔者认为:当人工智能不再只是“创作”的辅助工具(如:仅按照既定规则对素材编排、计算或剪辑),而能自主生成与现有表达不同的内容,体现特有的选择、编排或思想时,其生成物便可视为具有独创性。

综上,笔者认为,在一定条件下,人工智能生成物是可以符合著作权法规定的独创性要件的。

(二) 作者是否必须是“人”

对作品以著作权加以保护,是社会对创作者的褒奖。依照著作权法的规定,著作权属于作者,而创作作品的公民是作者。由法人或者其他组织主持,代表法人或者其他组织的意志创作,并由法人或者其他组织承担责任的作品,法人或者其他组织视为作者。

人工智能技术的进步会使得人工智能更智能、更独立,甚至具备某些人类的特征。但是,在可以预见的时期内,赋予人工智能人格权仍遥不可及,人工智能本身尚不能成为著作权法下适格的作者。美国曾出现过一个有趣的案例,一只黑猩猩使用摄影师的相机拍摄了几张自拍照,这几张自拍照因著作权权属问题引发诉讼。2015年,美国版权局专门发布了最新政策纲要,声明只有人创作的作品才可以拥有版权,特别规定任何动物的作品都不具备可版权的资格(不管是猴子的自拍照还是大象的壁画)。

在人工智能生成物满足作品所有构成要件的情况下,其作者仍必须

1. 该案案号为：
(2018)京0491民初
239号，北京互联网
法院于2019年4月25
日对该案作出一审判
决。

是“人”（自然人或法人）。基于此，笔者认为，要在具体场景下，考察人工智能“创作”生成物的具体过程，从而判断是否赋予对“创作”过程具有智力性贡献的“人”以著作权。需要明确，考察的对象是人工智能生成物而非人工智能程序本身，人工智能程序开发者对人工智能程序本身拥有著作权，但不一定对人工智能生成物享有著作权。

SECTION 003

人工智能生成物是否具有可版权性的司法实践现状

目前，我国司法实践中对于人工智能生成物是否具有可版权性这一问题尚未形成统一认识。例如：在菲林律所诉百度公司著作权侵权案中，北京互联网法院认为，即使涉案数据库分析报告具有独创性，由于自动生成涉案数据库分析报告的数据库软件不是自然人，因此，涉案数据库分析报告不是作品。然而，在某互联网公司A诉上海某科技公司B侵害著作权及不正当竞争案中，广东省深圳市南山区人民法院则认为人工智能生成物受到著作权法的保护。

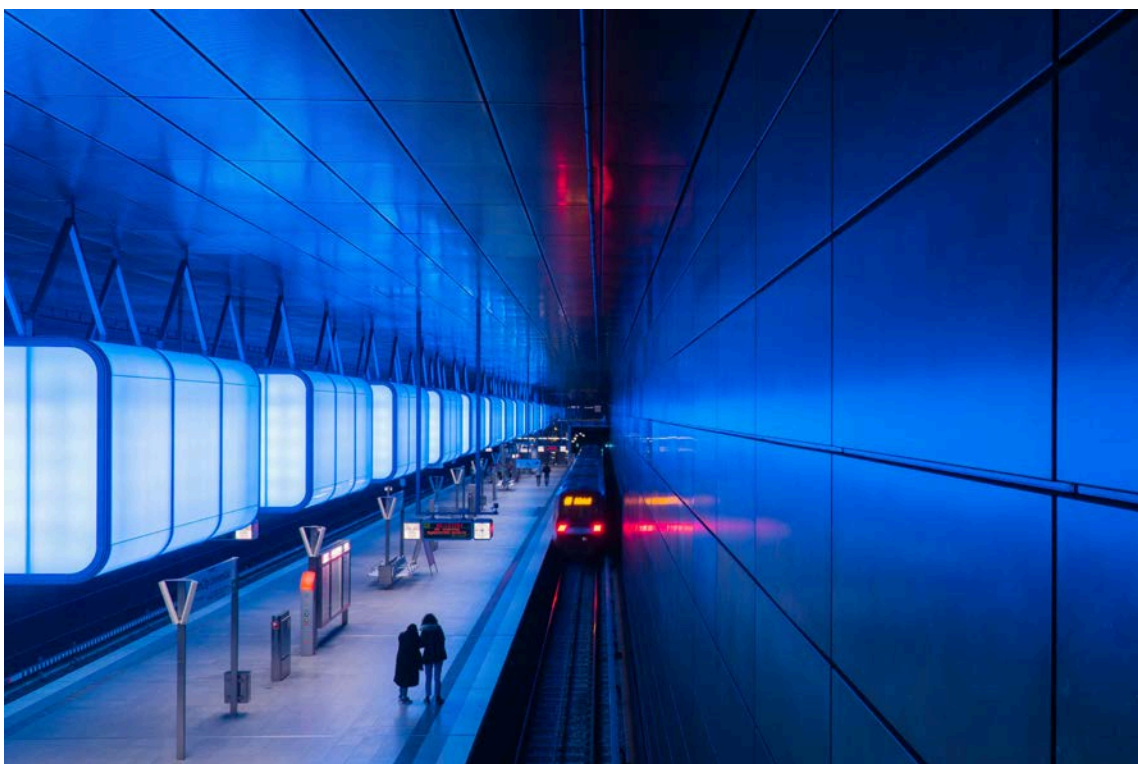
（一）案例一：菲林律所诉百度公司著作权侵权案¹

1. 案情概要

2018年9月9日，原告北京菲林律师事务所在其微信公众号上发表《影视娱乐行业司法大数据分析报告——电影卷·北京篇》（“涉案文章”）。涉案文章含有图表和数据，相关图表的基础图形是由威科先行库生成的，相关数据的基础数据来源于威科先行库生成的检索结果（威科先行库生成的图形和数据统称“数据库分析报告”）。2018年9月10日，被告百度公司未经许可在其经营的百家号平台“点金圣手”上发布涉案文章，并删除了涉案文章的引言、检索概况、电影行业案件数量年度趋势图和结尾的“注”部分及涉案文章的署名。原告认为被告的有关行为侵犯了其就涉案文章享有的信息网络传播权、保护作品完整权、署名权，遂将被告诉至北京互联网法院。

2. 法院观点

判定原告是否为适格主体，其实质是判定涉案文章是否构成作品、原告对涉案文章是否享有著作权。就该问题，法院主要审理了以下两方面：（1）是否具有独创性；（2）是否为自然人创作。就上述两个审理要点，法院认为，具备独创性并非构成作品的充分条件，自然人创作完成仍应是构成作品的必要条件。



(1) 是否具有独创性

经审理,法院认为,从数据库分析报告的生成过程看,选定相应关键词,使用“可视化”功能自动生成的数据库分析报告,其内容涉及对电影娱乐行业的司法分析,符合文字作品的形式要求,涉及的内容体现出针对相关数据的选择、判断、分析,具有一定的独创性。

(2) 是否为自然人创作

关于数据库分析报告是否为自然人创作这一问题,法院持否定态度,其审理逻辑概述如下:

首先,数据库分析报告系威科先行库利用软件使用者输入的关键词与算法、规则和模板结合形成的,因此,威科先行库在某种意义上“创作”了该分析报告。但由于威科先行库不是自然人,即使威科先行库“创作”的数据库分析报告具有独创性,该数据库分析报告仍不是作品,威科先行库亦不是作者。

其次,尽管软件开发者(所有者)、软件使用者作为自然人分别参与了数据库分析报告生成过程中的软件开发环节、软件使用环节,然而,由于数据库分析报告未有传递软件开发者(所有者)、软件使用者的思想、感情的独创性表达,该数据库分析报告不应被认定为由软件开发者(所有

者)、软件使用者创作完成。具体而言:(1) 软件开发者(所有者)未根据其需求输入关键词进行检索,数据库分析报告未传递软件开发者(所有者)的思想、感情的独创性表达,故软件开发者(所有者)不是作者;(2) 软件使用者仅提交了关键词进行搜索,数据库分析报告未传递软件使用者思想、感情的独创性表达,故软件使用者亦不是作者。

关于数据库分析报告的署名问题,法院认为,无论是软件开发者(所有者)还是软件使用者,非创作者均不能以作者身份署名。尽管如此,法院指出,从保护公众知情权、维护社会诚实信用和有利于文化传播的角度出发,可在数据库分析报告中添加生成软件的标识,标明系软件自动生成。

此外,虽然数据库分析报告不构成作品,但不意味着其进入公有领域后可被公众自由使用。法院认为,数据库分析报告的产生既凝结了软件开发者(所有者)的投入,也凝结了软件使用者的投入,具备传播价值。如果不赋予投入者一定的权益保护,将不利于对投入成果的传播,进而无法发挥其效用。但至于赋予投入者何种权益保护,法院在本案判决中未予以评析。

(二) 案例二:某互联网公司A诉上海某科技公司B侵害著作权及不正当竞争案²

广东省深圳市南山区人民法院受理的某互联网公司A诉上海某科技公司B侵害著作权及不正当竞争案亦涉及人工智能生成物是否具有可版权性这一问题。

原告A公司诉称,A公司智能写作助手完成的内容系由原告主持,代表原告意志创作,并由原告承担责任的作品,原告依法应视为A公司智能写作助手完成的内容的作者,该内容的著作权亦应归原告。被告B公司在其运营的“某贷之家”网站向公众传播A公司智能写作助手完成的内容,原告认为被告的行为侵犯了其信息网络传播权。

根据《法制日报》2020年1月2日的报道³,广东省深圳市南山区人民法院近期对该案作出了一审判决,一审原告胜诉。法院认为,涉案文章由原告主创团队人员运用A公司智能写作助手软件生成,其外在表现符合文字作品的形式要求,其表现的内容体现出对相关股市信息、数据的选择、分析、判断,具有一定的独创性。法院同时认为,涉案文章是由原告主持的多团队、多人分工形成的整体智力创作完成了作品,整体体现了原告的需求和意图,是原告主持创作的法人作品。进而认为被告侵害了原告享有的信息网络传播权。

2.目前该案判决原文尚无法从公开渠道获得,该案案号及具体的判决内容尚无法获知。

3.参见:
<https://mp.weixin.qq.com/s/sZN07FlISC-lNeyO5MwRAA>,最后访问时间:2020年2月25日。

上述两案件中,法院就人工智能生成物是否具有可版权性这一问题判决的迥异,可能并不代表法院在法律理解上的差异,或许主要源于两法院对各自案件事实认定的不同。案件一的法院认定各方(软件开发者、软件使用者)在数据库分析报告生成过程中没有智力型的贡献,数据库分析报告中没有传递他们的思想、感情的独创性表达;而案件二,法院认定了涉案文章是由原告A公司主持的多团队、多人分工形成的整体智力创作完成的作品,整体体现了原告A公司的需求和意图。

SECTION 004

著作权法外人工智能生成物可能的法律保护路径

通过著作权法获得保护,仅是人工智能生成物的保护路径之一。在现有法律框架下,若人工智能生成物无法获得著作权法的保护,人工智能的所有者可考虑通过如下两种保护路径对人工智能生成物进行法律保护。

(一) 通过合同法保护

人工智能程序所有者对人工智能生成物享有的特定权益在无法通过著作权法保护的情况下,仍可以通过合同法获得一定程度的保护。如:人工智能程序所有者可以通过其与相对方的合同(如:与该人工智能程序相关的商业合同或用户协议等)来限制第三方使用和传播人工智能生成物,若合同相对方违反约定,其将承担相应的违约责任。受限于合同关系的相对性,此路径的保护亦有一定局限性,如:不能对抗合同关系之外的第三方。

(二) 通过反不正当竞争法保护

根据具体情形,人工智能程序所有者还可以考虑通过反不正当竞争法就其对人工智能生成物享有的权益进行保护。由于人工智能生成物的产生凝结了人工智能程序所有者的投入,人工智能程序所有者对人工智能生成物应当享有一定的权益。在特定场景下,人工智能生成物将成为人工智能程序所有者通过一系列创造性劳动所累积形成的竞争优势,如果法律不禁止第三方对其擅自复制、转载、传播行为,将会使得竞争失序,利益失衡,有违诚实信用的基本竞争法则。



在现有的著作权法框架下，只有人工智能生成物具备独创性时，其才能获得保护。

4. 该决议于2019年9月18日作出, 报告原文详见: https://aip-pi.org/wp-content/uploads/2019/10/Resolution_Copy-right_in_artificially_generated_works_English1.pdf, 最后访问时间: 2020年2月25日。

(三) 通过专门立法予以规制

人工智能是新事物, 必然带来新的法律问题和挑战, 通过专门立法的方式予以调整亦是很自然的思路。以计算机软件和数据库为例, 其出现时也对传统的著作权法带来了不小的挑战, 虽然世界各国仍基本把计算机软件和数据库纳入到著作权法调整的框架内, 但鉴于其本质上与文字作品的差异, 很多国家已通过专门立法的方式对其保护给予专门规定, 以响应技术的发展。

通过专门立法的方式进行规制优势明显: 一是可以扩大人工智能生成物的保护范围(如: 将人工智能程序产生的数据纳入保护范围), 而不再拘泥于具有可版权性的作品; 二是可以有效平衡各方的利益关系, 使得人工智能程序开发者、人工智能程序应用者以及公众各得其所, 促进人工智能产业的发展。

SECTION 005

人工智能生成物的国际观点

国际保护知识产权协会 (“AIPPI”) 在2019年伦敦世界知识产权大会上发布了《人工智能生成物的版权问题决议》⁴, 该决议旨在: (1) 说明有关人工智能的问题中涉及版权领域的内容; (2) 确定人工智能生成物是否享有版权和/或邻接权, 以及在何种情况下享有版权和/或邻接权。

就人工智能生成物版权保护问题, AIPPI决议的基本观点如下:

(1) 统一或协调对人工智能生成物的保护是有必要的;

(2) 人工智能生成物只有在其生成过程有人类干预的情况下, 且在该生成物符合受保护作品应满足的其他条件的情况下, 才能获得版权保护。对于生成过程无人类干预的人工智能生成物, 其无法获得版权保护。

笔者认为, AIPPI决议就人工智能生成物的版权保护问题的有关观点体现了最新的国际保护趋势, 对探索人工智能生成物的保护路径有一定的参考意义。

SECTION 006

总结及展望

综上, 笔者对于人工智能生成物赋予著作权保护持有以下的观点:

(1) 在现有的著作权法框架下, 只有人工智能生成物具备独创性时, 其才能获得保护。简单的对数据的收集、排列或剪辑, 或基于固定算法的

分析计算,不构成著作权法保护的客体;

(2) 著作权法所保护的客体是人类智力型活动的成果,人工智能生成物的“创作”过程中须有人类智力型活动的参与才能获得著作权保护。因此,只有人工智能生成物反映了人类的思想、感情或观点,才能成为著作权法保护的客体;

(3) 考虑各方在人工智能生成物中的智力贡献,人工智能程序的开发者、应用者和既有作品的作者(如果人工智能生成物的“创作”利用了既有作品)均可能对人工智能生成物拥有一定的权益;

(4) 考虑到人工智能技术的快速发展,对人工智能生成物的保护已经超出了著作权的范畴(如:人工智能程序生成的机器数据),单独依赖著作权法对人工智能生成物进行保护已经显得不能适应,通过专门立法予以解决应当是一个恰当的思路。

总之,人工智能在“创作”领域深化应用的趋势已不可逆转,如何保护人工智能生成物是无法回避的问题。是选择既有著作权法的法律体系,还是寻求著作权法以外其他法律的保护,是不同的路径选择。面对不同的路径选择,加快关于人工智能生成物的相关立法及统一司法实践中的审判尺度非常必要。





2

CHAPTER 03

科技企业的上市中 知识产权风险的防范

作者:张诗伟/蔡鹏/李硕/潘聪

夫未战而庙算胜者,得算多也;未战而庙算不胜者,
得算少也。多算胜,少算不胜,而况于无算乎!

—《孙子兵法·计篇》

PART I 境内篇

以高科技为技术特征的新经济时代,某种意义上也是以知识产权为法律特征的新经济时代。资本市场作为新经济的金融机枢,尤其重视上市企业的知识产权合规问题。不少企业在申请上市的漫漫征途中因为该问题倒在了最后一公里,甚至即使在成功上市后因该问题而被处罚甚至退市。本文从案例实证分析角度分析了知识产权诉讼争议对中国上市公司/拟上市公司的影响,总结了相关知识产权诉讼频发的原因和特点,概括了企业在知识产权诉讼事项方面的相关证券合规要点,并建议企业在发起或应对知识产权诉讼前都应做好充分研究和应对的准备,不打无准备之仗,并进一步给出相关具体应对策略和合规建议。

SECTION 001

上市公司/拟上市公司知识产权诉讼的典型案列

(一) 拟上市企业知识产权争议案例实证

受精力和成本费用所限,企业在初创时期为了生存只关注业务,一心为产品或服务的拓展,而忽略了知识产权风险,从而为后期留下隐患。而随着发展壮大过程中随之而来的问题是在发展过程中时常会面临知识产权诉讼争议,而给企业的上市之路带来不确定性,也给投资人或企业融资之路带来不利的影响。企业飞速发展之后,在拟上市的敏感时期也经常面临知识产权诉讼争议,一旦处理不当,则势必会影响企业的上市进程。近几年颇受关注的IPO进程中与知识产权相关的案件如下表所示。

企业名称	争议对方	争议案由	涉案金额	诉讼日期	争议结果
乔丹体育	迈克尔·乔丹	商标争议 商标无效		2012/02	停止IPO
友利控股	威尔乌集团	著作权、商标 和不正当竞争	3100万	2015/09	中清龙图借壳 上市失败
传音控股	华为	著作权侵权	2000万	2019/09	已上市,未有效 应对,股价下挫
松德股份	仕诚公司	专利争议 投诉举报		2010/06	经解释后过会

企业名称	争议对方	争议案由	涉案金额	诉讼日期	争议结果
安翰科技	金山科技	专利侵权	5000万	2019/05	终止审核
白山科技	网宿科技	专利侵权	1.5亿	2019/05	中止审核
晶丰明源	矽力杰	专利侵权	400万	2019/07	有效应对
公牛集团	通领科技	专利侵权	10亿	2018/12	有效应对

独角兽相关的知识产权案件实证

独角兽企业作为相关行业的头部企业,其涉及的知识产权争议问题无疑也非常值得关注,下表收集了近年来发生的相关知识产权争议案例。

企业名称	争议对方	争议案由	涉案金额	诉讼日期	争议结果
滴滴出行	杭州妙影	商标侵权	8000万	2014/05	更改名称
重庆江小白	重庆江津	商标无效		2016/05	保住商标
唐德影视	上海灿星	商标和不正当竞争	5.1亿	2016/06	和解
传奇时代	山东机客网络	著作权纠纷	36万	2014/08	二审胜诉
摩拜单车	深圳吟云	专利侵权	130万	2017/03	专利无效
小狗电器	戴森	专利侵权	100万	2017/09	诉讼中
绿米科技	西门子	专利侵权	600万	2018/09	一审败诉
科沃斯	戴森	专利侵权	100万	2014/09	二审胜诉

(二) 上市公司典型知识产权争议案例实证

企业上市之后,其作为上市公司在面临激烈的市场竞争时也会主动或被动地参与到与知识产权相关的争议案件中,近年来广泛关注的知识产权方面的争议案件如下表所示。

企业名称	争议对方	争议案由	涉案金额	诉讼日期	争议结果
光峰科技	台达电子	专利侵权	4843万	2019/07	有效应对, 股价上涨
格力电器	奥克斯	专利侵权	4600万	2017/11	主动维权
美的电器	云米科技	专利侵权	400万	2018/06	主动维权
长阳科技	日本东丽	专利侵权	2600万	2019/11	未有效应对, 股价下挫
金象赛瑞	华鲁恒升	专利侵权、商业秘密	2.33亿	2017/08	主动维权
平安健康	好医生药业	商标侵权	9000万	2018/04	未有效应对, 股价下挫
广药集团	加多宝	商标、包装装潢侵权和不正当竞争	14.4亿	2012/03	主动维权
北大方正	暴雪娱乐	著作权侵权	4.08亿	2007	主动维权
吉利控股	威马汽车	商业秘密	21亿	2018	主动维权
搜狗公司	百度公司	专利侵权	1亿	2015	主动维权

SECTION 002

上市公司/拟上市公司知识产权诉讼频发的原因和特点

(一)原因

由上,我们初步理解,企业在上市前、上市中和上市后都会产生大量知识产权诉讼争议,其原因主要包括市场竞争、被动防御、主动维权等方面的因素。

1、在市场竞争方面。在知识产权成为企业核心竞争力的时代,企业之间的竞争实际上就是知识产权的竞争。从全球化的角度而言,主要的竞争主体都会在各国内布局大量的专利和商标等智慧财产。一旦竞争对手出于各种需要启动知识产权诉讼,则势必会产生大量的知识产权纠纷案件。比如戴森在无叶风扇、手持式吸尘器等方面拥有较强的技术实力并且在全球都布局有大量的专利,其针对小狗电器和科沃斯发起的专利侵权诉讼就是典型代表。

2、被动防御。知识产权等无形资产是企业的重要资产和防御对手的重要盾牌,由于企业经常会不由自主地陷入各种知识产权相关的纠纷之中,因此适时穿上知识产权所赋予的保护铠甲,会给企业在激烈的市场竞争中带来更有力的安全感。以光峰科技vs台达电子案为例,光峰科技

是激光投影领域的新秀,在面临对手的诉讼时积极作为,并且利用自有专利发起反诉以获得制衡,从而实现从被动防御到积极应对的良好转变。

3、主动维权。由于企业维权的需要或者企业在竞争中的策略需求,主动发起各种诉讼手段来维护合法权益是非常常见的合法手段。占据市场竞争优势、压制竞争对手、为自身争取技术突破和融资窗口等都是企业在主动维权时需要考量的因素。以搜狗公司vs百度公司案为例,搜狗公司在面对百度输入法的市场侵蚀时,主动选择发起大量专利侵权诉讼,该诉讼旷日持久,最终搜狗公司在数起诉讼中已经获得胜诉结果,在市场竞争中相对赢得主动。

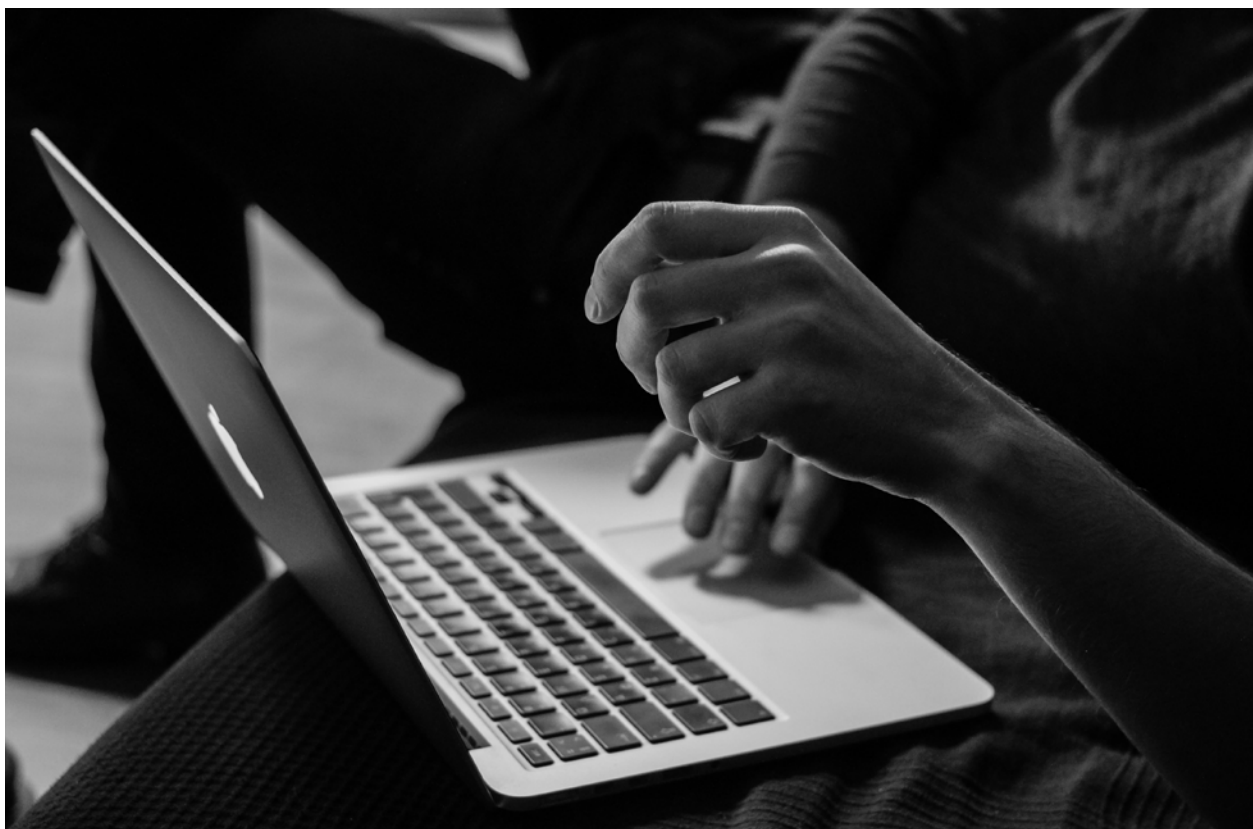
国内外的案例都表明,由于资本市场对于企业融资便利、巨大的财富效应以及强大的品宣效果,企业如抢得资本市场上市先机无疑通常可以获得相对的竞争优势。这通常使得竞争对手对此无法做到泰然处之,举报或提起知识产权争议诉讼就成为影响甚至阻遏对方顺利上市通常的手段。

(二)特点

从上表也可以出,知识产权诉讼呈现出涉案面广、涉及法域繁杂、参与主体众多、案件量日趋上升、赔偿额日益增长,保护力度加大等特点。

1、从涉案面来看,无论是传统行业(例如服装行业、机械制造、化工行业、电器行业、家具行业等,代表性企业如乔丹体育、公牛集团、格力电器、奥克斯、美的电器、金象赛瑞、广药集团、吉利控股等),还是新兴行业(例如计算机、通信、网络、区块链、AI,代表性企业如滴滴出行、摩拜单车、杭州骑客、小狗电器、科沃斯、传音控股、光峰科技、北大方正、搜狗、百度、腾讯、360等),都存在大量涉及知识产权方面的诉讼和争议案件。这也可以印证出在国家倡导建设创新型国家的大环境下,知识产权的保护已经深入人心,并渗透到各行各业中。

2、从涉及法域来看,目前知识产权诉讼争议包括了专利(例如搜狗vs百度、公牛vs通领科技、摩拜vs深圳吟云)、商标(例如滴滴出行vs杭州妙影、乔丹体育)、著作权(例如北京传奇vs机客网络、传音控股vs华为、北大方正vs暴雪娱乐)、商业秘密(例如吉利控股vs威马汽车、金象赛瑞vs华鲁恒升)、不正当竞争(例如腾讯公司vs360公司)、包装装潢(例如广药集团vs加多宝)、权属争议(例如江小白vs重庆江津)、反垄断等各个方面。由于知识产权诉讼涉及法域繁杂,因此对代理案件的律师提出了更高的专业要求。



3、从参与主体来看,目前知识产权案件主要涉及自然人/企业/行业协会、律师/专利代理师、政府行政部门、以及法院等多种主体。例如针对专利和商标纠纷,由于诉讼争议的过程中经常会涉及政府行政部门的确权争议,因此导致多种主体参与到诉讼案件的解决中(例如光峰科技vs台达电子案、搜狗公司vs百度公司案中涉及大量的专利无效行政程序)。目前法院为解决审判尺度一致的问题,也引入了行政诉讼和侵权诉讼合并审理的制度,并普遍推广知识产权“三审合一”审判体系,提升权利人维权的便捷程度和效率,这也是企业在面临知识产权诉讼争议时需要关注的发展方向。

4、从案件量来看,无论是商标诉讼、专利诉讼,还是著作权和不正当竞争诉讼,都呈日趋上升的趋势,这也从侧面反映出目前企业主体日益懂得利用知识产权诉讼争议来维护自身的权益的现实。

5、从赔偿额来看,目前在鼓励创新和惩治抄袭的大背景下,平均赔偿额日益增长(例如广药集团vs加多宝判赔高达14.4亿),知识产权强保护力度持续加大。特别地,商标法中早已引入惩罚性赔偿制度,而目前修改中的专利法也正在讨论该制度的引入。

SECTION 003

上市公司/拟上市公司在知识产权诉讼相关证券监管要点**(一) 拟上市企业涉及知识产权诉讼相关上市条件及申报披露要求**

拟上市公司知识产权的纠纷及诉讼情况,是判断及核查其是否符合企业资产是否完整以及是否具有持续经营能力法定的发行上市条件之一,如触发上市条件,则其直接构成上市的实质性法律障碍而上市之路就此阻断。即使其不触发发行上市条件,其对发行上市的影响和足够的披露也是证券监管部门重点关注的问题。因此,企业在申请上市的过程中,应当特别注意对知识产权的保护以及纠纷、潜在纠纷的应对和处理以及相关上市申报文件的披露。

1、上市条件

《证券法》(2019年修订)第十二条规定:“公司首次公开发行新股,应当符合下列条件:(二)具有持续经营能力。”知识产权作为拟上市公司的核心资产之一,是拟上市公司保障其持续经营能力的重要要素,历来受到上市监管机关的重视。监管机关对于拟上市企业知识产权诉讼的关注,主要着眼于其对企业持续经营能力的影响。这一思路也贯穿于中国证监会、交易所出具的各项文件中。《首次公开发行股票并上市管理办法(2018年修正)》第十三条规定,发行人不得有下列影响持续经营能力的情形:(五)发行人在用的商标、专利、专有技术以及特许经营权等重要资产或技术的取得或使用存在重大不利变化的风险。第二十八条规定:发行人不存在重大偿债风险,不存在影响持续经营的担保、诉讼以及仲裁等重大或有事项。《首次公开发行股票并在科创板上市管理办法(2018年修正)》第十二条规定:发行人的主要资产不存在重大权属纠纷。《科创板首次公开发行股票注册管理办法(试行)》第三条规定,发行人申请首次公开发行股票并在科创板上市,应当符合科创板定位,拥有关键核心技术、主要依靠核心技术开展生产经营。该办法第十二条规定,发行人申请股票在科创板上市,应当满足“发行人业务完整,具有直接面向市场独立持续经营的能力”,其中包括“资产完整”“发行人不存在主要资产、核心技术、商标等的重大权属纠纷”等具体条件。

中国证监会于2019年3月25日发布的《首发业务若干问题解答》以及上海证券交易所于2019年3月24日发布的《上海证券交易所科创板股票发行上市审核问答(二)》中,也都将“对于发行人业务经营或收入实现有重大影响的商标、专利、专有技术以及特许经营等重要资产或技术存在

重大纠纷或诉讼,已经或者未来将对发行人财务状况或经营成果产生重大影响”作为核查判断发行人是否存在影响持续经营能力的情况的主要标准。

2、上市申报文件披露要求

《公开发行证券的公司信息披露内容与格式准则1号——招股说明书》第一百二十六条规定:发行人应披露对财务状况、经营成果、声誉、业务活动、未来前景等可能产生较大影响的诉讼或仲裁事项,主要包括:(一)案件受理情况和基本案情;(二)诉讼或仲裁请求;(三)判决、裁决结果及执行情况;(四)诉讼、仲裁案件对发行人的影响。《公开发行证券的公司信息披露内容与格式准则第41号—科创板公司招股说明书》第六十二条规定,发行人应分析披露其具有直接面向市场独立持续经营的能力:(七)发行人不存在主要资产、核心技术、商标的重大权属纠纷,重大偿债风险,重大担保、诉讼、仲裁等或有事项。该准则第九十六条规定,发行人应披露对财务状况、经营成果、声誉、业务活动、未来前景等可能产生较大影响的诉讼或仲裁事项,主要包括:(一)案件受理情况和基本案情;(二)诉讼或仲裁请求;(三)判决、裁决结果及执行情况;(四)诉讼、仲裁案件对发行人的影响。《公开发行证券公司信息披露的编报准则第12号—公开发行证券的法律意见书和律师工作报告》第四十九条规定,如发行人、持有发行人5%以上的主要股东、发行人的控股公司存在尚未了结的或者可预见的重大诉讼、仲裁及行政处罚案件的,应当对案件的简要情况作出说明(包括但不限于受理该案件的法院名称、提起诉讼的日期、诉讼的当事人和代理人、案由、诉讼请求、可能出现的处理结果或已生效法律文书的主要内容等),并说明对公司股票发行、上市的影响。

3、监管机关反馈及问询要点

近期A股IPO审核过程中,监管机关反馈及问询问题中涉及发行人知识产权纠纷、诉讼或仲裁的部分案例,监管机关主要关注发行人报告期内知识产权诉讼的金额、背景、诉讼进程、知识产权诉讼与发行人业务、产品的关系、知识产权诉讼对发行人资产完整性、持续经营能力的影响等事项,具体反馈意见如下:

公司简称	上市板块	反馈问题	上市审核状态
上能电气股份有限公司	创业板	(发行人多名董事、核心技术人员曾在同行业公司艾默生任职), 请说明发行人报告期内是否存在知识产权纠纷或诉讼, 如存在, 请披露具体情况。	已过会
广州市浩洋电子股份有限公司	创业板	(发行人下属子公司曾与飞利浦集团签署专利授权协议) 请补充披露海外专利的具体性质、报告期内是否存在专利纠纷、诉讼等情形。	已过会
常州凯迪电器股份有限公司	主板	(招股书披露, 某原告向德国杜塞尔多夫法院提起专利侵权诉讼, 将包括发行人在内的三方主体作为共同被告) 请补充披露上述诉讼的最新进展情况, 是否满足预计负债的确认条件, 上述诉讼的主张金额及对发行人生产经营及财务情况的影响。	已反馈
北京万泰生物药业股份有限公司	主板	(发行人两项专利存在专利诉讼情况) 请保荐机构、发行人律师核查并披露: (1) 该等专利权利人的情况; (2) 该等专利与发行人生产经营的关系; (3) 该等专利所涉诉讼事项对发行人持续经营的影响, 未在招股书中披露该等专利所涉诉讼事项的原因; (4) 发行人募投项目是否需要使用上述专利, 是否可能侵犯上述专利权利人的权利。	已反馈
浙江双飞无油轴承股份有限公司	创业板	请发行人说明各项专利的取得方式、核心技术的来源及形成、发展过程; 是否涉及董事、监事、高级管理人员或其他核心人员在曾任职单位的职务成果, 是否存在权属纠纷或潜在纠纷; 发行人报告期内是否存在知识产权纠纷或诉讼, 如存在, 请披露具体情况。	已过会
北京盈建科软件股份有限公司	创业板	(发行人报告期内曾作为被告涉及计算机软件著作权诉讼, 后以原告申请撤诉结案) 请发行人说明上述诉讼中原告的诉讼请求及主要事实与理由, 原告撤诉的原因, 是否与发行人签署和解协议, 如是, 请说明协议的主要内容; 发行人及其实际控制人与原告之间是否存在与该诉讼有关的其他协议或类似安排, 发行人关联方是否存在代发行人向原告承担或承诺承担赔偿责任或补充义务的情形; 请说明发行人与国内外主要竞争对手、同行业公司或其他主体间是否存在知识产权相关的诉讼、仲裁或其他纠纷。	已反馈
安徽芯瑞达科技股份有限公司	中小板	请发行人补充披露核心技术对第三方是否存在依赖, 是否存在诉讼、纠纷或其他引致权利不确定性的情况, 是否影响发行人的资产完整性, 是否构成本次发行上市的法律障碍。	已反馈

公司简称	上市板块	反馈问题	上市审核状态
安克创新科技股份有限公司	创业板	据招股说明书披露,发行人除知识产权诉讼外,还存在拥有 574 项国内注册商标,其中 6 项商标权涉及争议或纠纷。请发行人:补充披露相关商标权的具体使用用途、范围及实现收入占比,并据此分析说明相关诉讼结果或评审结果对发行人生产经营的具体影响、是否影响发行人的资产完整,并充分提示相应风险;补充说明截至目前,发行人、控股股东、实际控制人、董监高、其他核心人员是否涉及其他未披露的重大诉讼或仲裁事项。	已反馈
北京新时空科技股份有限公司	中小板	招股说明书披露,发行人拥有 3 项注册商标、17 项专利、14 项计算机软件著作权。报告期内,发行人与北京工业大学存在合作研发。请发行人进一步说明:是否存在利用关联方或非关联方的职务发明的情形,核心技术对第三方是否存在依赖,是否存在诉讼、纠纷或其他引致权利不确定性的情况,是否影响发行人的资产完整性,是否构成本次发行上市的法律障碍。	已反馈
奥锐特药业股份有限公司	主板	请发行人补充披露:(1) 发行人专利技术的形成过程、取得方式,各专利发明人与发行人的关系,是否存在权属纠纷;(2) 关于 ZL97197460.8 号专利的诉讼进展情况,发行人涉及该专利的产品的销售情况,如果最高人民法院判决专利复审委败诉将对发行人生产经营和财务情况产生的具体影响。	已反馈
湖南南新制药股份有限公司	科创板	请说明发行人核心技术及专利的形成过程,关联方拥有或使用与发行人业务相关的商标、专利等知识产权的情况,是否存在对核心技术人员的依赖,是否与其他机构或研发人员存在纠纷及潜在纠纷。	注册生效
安翰科技(武汉)股份有限公司	科创板	近期出现多篇针对发行人的媒体质疑报道(主要涉及专利诉讼)。请发行人、保荐机构、发行人律师和申报会计师对相关报道所涉事项进行核查,并发表明确意见。	终止申请
浙江东方基因生物制品股份有限公司	科创板	发行人境外子公司美国衡健存在一起境外专利涉诉案件:W.H.P.M.,Inc于2018年7月起诉美国衡健侵犯其编号为 7927562 的专利权,案件已被德克萨斯州南部地区美国地方法院受理,该案尚在庭前证据交换披露阶段。请发行人补充披露:该案基本案情、诉讼请求、具体涉诉的金额,可能受该案影响的发行人及其子公司产品的具体情况,该案件对发行人及其子公司生产经营的具体影响。	注册生效

根据上述反馈意见,可以看出,监管机关在企业上市申请主要关注知识产权诉讼的以下要点:

(1)如发行人存在数量较多的专利权、商标权等知识产权,或发行人存在合作研发、共有知识产权等特殊情况,或发行人核心技术人员曾在发行人合作方、同行业竞争对手任职的情况的,则监管机关对于发行人的知识产权诉讼情况会给予更多关注,要求其全面披露报告期内的知识产权诉讼情况,而不论相关诉讼的金额上是否达到重大诉讼标准;

(2)如发行人报告期内存在知识产权诉讼情况的,除需要披露该诉讼的基本情况外,监管机关还会要求发行人及中介机构就该知识产权与发行人业务、产品的关系、该诉讼对于发行人业务的实际影响发表明确意见;

(3)即便发行人报告期内发生的知识产权诉讼已经完结(如通过原告撤诉、和解等方式),依然存在监管机关要求披露该等诉讼的相关情况的可能性,并进一步要求披露撤诉、和解的原因及相关安排;

(4)监管机构问询的最终落脚点都为知识产权诉讼对于发行人资产完整性、持续经营能力的影响。

(二)上市公司知识产权诉讼事项披露的关注要点

企业上市后,需遵循中国证监会、证券交易所一系列信息披露要求,及时披露对于上市公司重要的信息。根据《证券法》(2019年修订)的相关规定,上市公司在涉及公司的重大诉讼、仲裁等重大事件时需要向国务院证券监督管理机构和证券交易场所报送临时报告,并予公告,说明事件的起因、目前的状态和可能产生的法律后果。

《上市公司信息披露管理办法》进一步规定,上市公司年度报告、中期报告应当披露报告期内重大事件(包括重大诉讼、仲裁等)及其对公司的影响。该办法第三十条规定,如发生可能对上市公司证券及其衍生品种交易价格产生较大影响的重大事件(包括涉及公司的重大诉讼、仲裁),投资者尚未得知时,上市公司应当通过临时公告的方式立即披露,说明事件的起因、目前的状态和可能产生的影响。此外,还应当持续披露该诉讼、仲裁的重大进展和结果。《上海证券交易所股票上市规则》《上海证券交易所科创板股票上市规则》《深圳证券交易所股票上市规则》《深圳证券交易所创业板股票上市规则》等,均较为详细的规定了需披露的诉讼、仲裁事项的披露标准,具体如下:

序号	上市板块	金额标准及披露要求	是否连续12个月累积计算状态	向交易所提交的文件	需披露的文件及信息
1	上交所主板	(一) 涉案金额超过1000万元, 并且占公司最近一期经审计净资产绝对值10%以上; (二) 董事会认为可能对公司股票及其衍生品种交易价格产生较大影响的; (三) 交易所认为必要的。	是	(一) 公告文稿; (二) 诉状或者仲裁申请书、受理(应诉)通知书; (三) 判决或者裁决书; (四) 交易所要求的其他材料	(一) 案件受理情况和基本案情; (二) 案件对公司本期利润或者后期利润的影响; (三) 公司及控股子公司是否还存在尚未披露的其他诉讼、仲裁事项; (四) 交易所要求的其他内容; (五) 重大进展情况及其对公司的影响, 包括但不限于诉讼案件的初审和终审判决判决结果、仲裁裁决结果以及判决、裁决执行情况。
2	上交所科创板	(一) 涉案金额超过1000万元, 且占公司最近一期经审计总资产或者市值1%以上... (三) 董事会认为可能对公司控制权稳定、生产经营或股票交易价格产生较大影响的其他诉讼、仲裁。 上市公司的核心商标、专利、专有技术、特许经营权或核心技术许可丧失、到期或出现重大纠纷, 应当及时披露其对公司核心竞争力和持续经营能力的具体影响。	未明确规定	未明确规定	未明确规定
3	深交所主板、中小板	同1	是	同1	同1
4	深交所创业板	除涉案金额改为超过500万元, 其余同1。 上市公司出现下列致使公司的核心竞争能力面临重大风险情形之一的, 应当及时向本所报告并披露: 公司在用的商标、专利、专有技术、特许经营权等重要资产或者技术的取得或者适用发生重大不利变化。	是	同1	同1

SECTION 004

上市公司/拟上市公司知识产权风险的应对策略和合规建议

(一) 拟上市公司知识产权诉讼事项应对策略建议

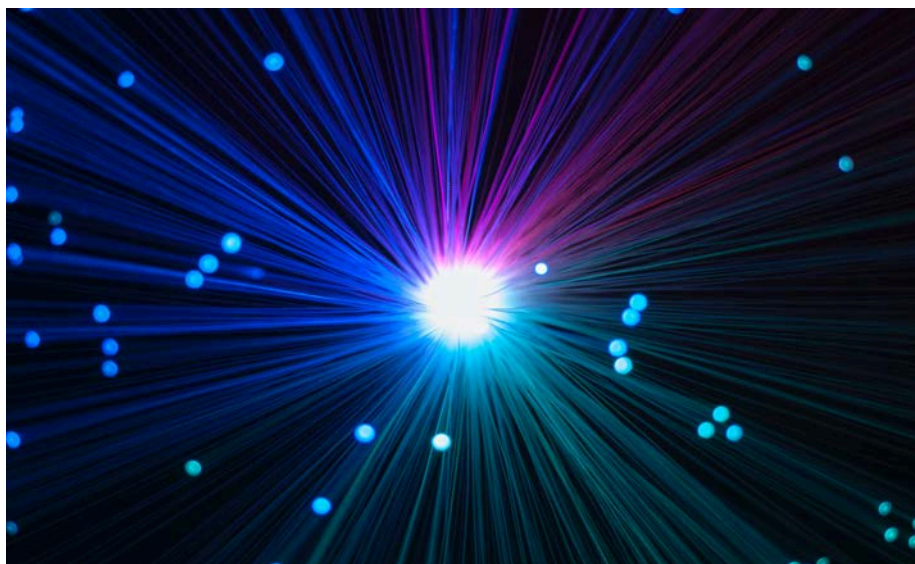
1、上市前应进行充分、全面的知识产权法律盘点、摸底或“体检”，尤其是针对于发行人主要业务及产品中使用的核心知识产权。摸底的目标是排雷。通过摸底发现核心无形资产中的瑕疵和问题，特别是企业的专利、专有技术、软件等技术类资产中，可能涉及到的权利归属、权利形成、权利处分以及流转中的瑕疵，由此可能存在的已有和潜在的知识产权争议诉讼。魔鬼经常在细节之中。一般的发行人律师角色可能都未必满足该需求，必要时建议聘请专门的知识产权（法律）顾问进行专项的核查。

2、尽量避免在上市前与任何第三方产生知识产权争议或纠纷或发生知识产权侵权行为，如存在相关风险或已产生相关争议，应尽早、积极与对方开展沟通与协商，争取达成和解，尽量避免争议升级成为正式的诉讼争议程序，从而把风险消除在萌芽甚至未萌状态。

3、主动面对和披露已发生的知识产权诉讼仲裁事项，积极回应市场与监管机构的疑问及质疑。对可能受到竞争对手的恶意诉讼或举报，或出现第三方借机讹诈的情况，在此种情况下，正常的沟通与协商显然已不可能。鉴于目前审核已更加市场化，并把握重大性原则而且对类似情形也非常了解，因此企业对此也不用惊慌失措，要冷静分析，沉着应对：（1）诉讼应对方面，在诉讼律师和知识产权顾问的协助下综合研判全面信息和局势，在此基础上有个预估预判和多种诉讼应对方案，进而提前锁定、固定相关证据并形成证据链；（2）上市申报方面，在上市法律顾问和知识产权顾问的协助下从行业、技术、事实证据、逻辑、胜诉可能性等多个角度对诉讼情况进行客观的阐释和披露，回应市场及监管机关可能产生的疑问与质疑，并避免挤牙膏式的披露而给审核部门留下不好不诚信的印象和给企业上市造成不利影响。

4、及早建立健全知识产权管理、保护体系和知识产权合规文化

知识产权的纠纷争议及其不利后果，说到底侵害的是企业的正常持续经营，以及自身的资产权属及核心竞争力。因此，不仅仅是出于顺利上市的目的，企业为了长远稳定发展，都有必要建立并实施一整套企业知识产权保护体系及护城河，实现合规经营，并有效的管理、识别、发现、预警、降低及化解知识产权风险。因此，企业不仅应当尽早建立健全的知识



产权管理、保护体系,而且须贯彻实施到企业的每个重要环节中,形成知识产权的合规文化。

(二)上市公司知识产权诉讼披露和应对策略建议

1、严格按证券法律法规规则履行上市公司的信息披露义务

作为上市公司,区别于非上市公司,需要多承担的法律义务最主要的莫过于前述法定信息披露义务。尤其值得注意的是新生效的《证券法》(2019年修订)大大加重了违反信息披露义务的法律后果。比如就行政法律责任而言,该法规定,对于上市公司信息披露违法行为,从原来最高可处以六十万元罚款,提高至一千万元;对于发行人的控股股东、实际控制人组织、指使从事虚假陈述行为,或者隐瞒相关事项导致虚假陈述的,规定最高可处以一千万元罚款。该法还同时完善了证券违法民事赔偿责任的规定,明确了发行人的控股股东、实际控制人在欺诈发行、信息披露违法中的过错推定、连带赔偿责任等。企业在上市成为上市公司后,对于知识产权诉讼的应对过程中,除正常应诉外,应当尤为注意信息披露的及时、完整与规范。而不同信息的披露格式、口径显然会产生不同的效果。企业应当在专业顾问的协助下,严格依据法律法规规则实事求是确定合法合规合适的披露格式,以尽可能降低对企业的不良影响。

在这个过程中,一方面对外要积极与交易所进行沟通。另一方面,在企业内部,也应当建议更高效的信息传递机制及知识产权应对机制,保证信息披露部门能从业务部门、财务部门以及资产管理、法律合规等部

门等及时、全面获得知识产权诉讼的相关信息，避免由于信息披露不合规收到相关行政处罚或监管措施，造成“二次伤害”。

2、积极、及时维权，多种方式并举实施应对方案

上市公司一旦发现其知识产权被侵犯，需要进行审慎的诉前评估，对于案件事实部分，以专利诉讼为例，需要考虑专利的稳定性、侵权产品是否容易获得、侵权赔偿额的计算、以及是否有恶意诉讼的风险等问题。对于案件策略，大到诉讼成本、取证方案、诉讼流程、管辖法院等基本问题，小到公证安排、律师函发出等细节问题，均需要通盘考虑以达到最优效果。上市公司主动维权应对（如积极应诉、谈判和解、反诉或另行起诉）的策略，是向资本市场释放出的积极信号，有利于让投资者和监管层对上市公司保持信心。

如企业在境外上市的，由于很多境外证券市场通常有严格的信息披露要求和成熟的集体证券诉讼制度，如企业信息披露不规范导致投资者权益受到损失的，除了受到行政处罚或监管措施外，还可能遭到大规模集体诉讼，不仅可能面临高额赔偿，对于企业的声誉及市场形象也可能遭受重创。因此也同样予以高度重视注意，前述相关防控措施亦同样适用。

PART II 境外篇

近日根据公司披露以及有关媒体报道，海能达通信股份有限公司（以下简称“海能达”）及全资子公司 HYTERA AMERICA, INC.（以下简称“美国公司”）、HYTERA COMMUNICATIONS AMERICA(WEST), INC.（以下简称“美西公司”）与 MOTOROLA SOLUTIONS INC.（以下简称“摩托罗拉”）、摩托罗拉马来西亚公司之间的商业秘密及版权侵权诉讼案件已于北京时间2020年2月15日由伊利诺伊州法院陪审团作出了裁决，根据摩托罗拉在庭审中的主张，海能达部分DMR产品侵犯摩托罗拉21项商业秘密及4项美国版权，要求海能达及相关被告就侵犯其商业秘密行为支付相应赔偿。近日，伊利诺伊州法院法官对本案作出一审判决，支持陪审团裁决结果，判决公司、美国公司及美西公司向摩托罗拉支付损害赔偿34,576.12万美元及惩罚性赔偿41,880万美元，合计76,456.12万美元（约合人民币53.34亿元）。根据预计，尽管总收入有增长，但上市公司海能达2019年度利润大幅下降，归属上市公司股东的净利润-47.75亿元，

如何通过海外知识产权诉讼的大考，将会是摆在中国本土上市公司面前一道刻不容缓的命题。

同比下降1101.41%。

跨境知识产权诉讼带给上市公司的影响之巨大,从海能达的案件中可见一斑。海能达案件并不是中国上市公司的个案,随着中国经济转型的深入,“一带一路”政策的影响,国际形势和商业环境的变化,以及本土企业全球化发展的趋势,此类上市公司的跨境知识产权诉讼将会越来越多。如何通过海外知识产权诉讼的大考,将会是摆在中国本土上市公司面前一道刻不容缓的命题。本文将通过研究近年来发生的境外典型案例,探究上市公司有关诉讼起因,并据此分析有关诉讼特点和监管趋势,为上市公司准备或应对海外的知识产权诉讼,抛砖引玉。

SECTION 001

上市/拟上市公司境外知识产权诉讼的统计

中国企业在上市前/拟上市/上市后都可能面临境外知识产权诉讼方面的争议。近年来,随着中国企业在全球市场中的表现日趋活跃,时常会面临竞争对手在境外发起的知识产权诉讼,这些年颇受关注的境内企业在海外发生的与知识产权相关的案件如下表所示。

企业名称	争议对方	争议案由	涉案金额	诉讼地域	争议结果
海能达	摩托罗拉	商业秘密和版权	53.34亿元人民币	美国	败诉
华锐风电	美国超导	商业秘密	约34亿元人民币	美国	和解
海信	博世	商标侵权	4000万欧元	德国	和解
深圳朗科	美国PNY	专利侵权	771万美元	美国	授权许可
迈瑞医疗	马西莫	专利侵权	2500万美金	美国	败诉
中兴	Maxell	专利侵权	4330万美元	美国	败诉
中国双环	德国宝马	外观设计专利侵权	每辆25万欧元赔偿	德国	败诉
通领科技	ITC	337调查		美国	有限排除令和禁止令
TCL	爱立信	标准必要专利诉讼	许可费	美国	诉讼中
海信	LG	标准必要专利诉讼	许可费	美国	诉讼中
海尔	Sisvel	标准必要专利诉讼	许可费	德国	和解
OPPO	杜比	标准必要专利诉讼	许可费	印度	和解

SECTION 002

上市公司/拟上市公司境外知识产权诉讼频发的原因

从上表中可以看出,中国企业主动或被动参与到境外知识产权诉讼的原因主要在于以下几个方面。

(一) 中国企业“走出去”和全球化布局带来的必然后果

越来越多国内企业走出去,带来的是商业市场全球化的布局。中国企业所到之处,必然要遵守所在国家的法律制度。知识产权法律体系虽然在某些基本概念方面大同小异,但是在具体的立法、执法和案件层面却大相径庭,这也是知识产权地域性特点所决定的。知识产权保护制度发端于欧洲,在欧美等发达国家已经存续上百年,其制度和执法体系对权利人的保护日趋完善。故在必要之时,发生知识产权诉讼以解决商业问题是十分常见的现象。以表中的美国超导和华锐风电的诉讼为例,双方的诉讼大战遍及美国、奥地利、巴西、北京以及海南等多个战场。近年来发生的高通和苹果在全球不同国家提起的专利侵权诉讼,也突出反映了企业全球化带来的诉讼全球化之特征,商业主体能够利用不同国家的知识产权保护特点,对竞争对手实施全球诉讼,以达到目标的有效策略。

(二) 缺乏战略思维导致问题频出

从某些案例可知,不排除某些企业在国内/国外商业活动中已经存在侵犯他人商业秘密、专利权等知识产权的行为,这些企业不仅没有警醒和采取补救措施,反而采取放任的态度。甚至,不乏有些案件中企业以违法的手段,以固有思维对他人的知识产权进行侵犯,最后导致严重后果。在有些重大的案件中,境外的法院已经对案件所涉关键事实(如盗窃商业秘密)进行了确认和判定,但是当战火逐步点燃,战场越大越大之时,企业不仅没有站在规则的角度去理性考虑,及时止损,反而利用其不当的力量去引导诉讼和争议往更坏的方向发展,失去了商业和解的宝贵机会,留下的则是“一地鸡毛”。

可以看出,将某些僵化的思维习惯应对知识产权的合规问题以及随之而来的跨境诉讼,不仅会对企业自身造成严重的损失和伤害,而且对整体行业以及国家形象形成次生危害。

(三) 企业知识产权合规的忽视而演变成诉讼风险

根据笔者对有关企业的观察和经验,即使该企业已经国际化经营很多年,也做了一些企业合规建设,但是在实施中考虑到成本等相关原因,缺乏必要的实施机制,导致对风险的识别能力不够而未发现隐藏在其中的知识产权风险,最后酿成跨境诉讼。特别是在全球供应链体系下,某一个合作伙伴所涉及的知识产权风险,有可能直接演变成对企业的不利诉讼。

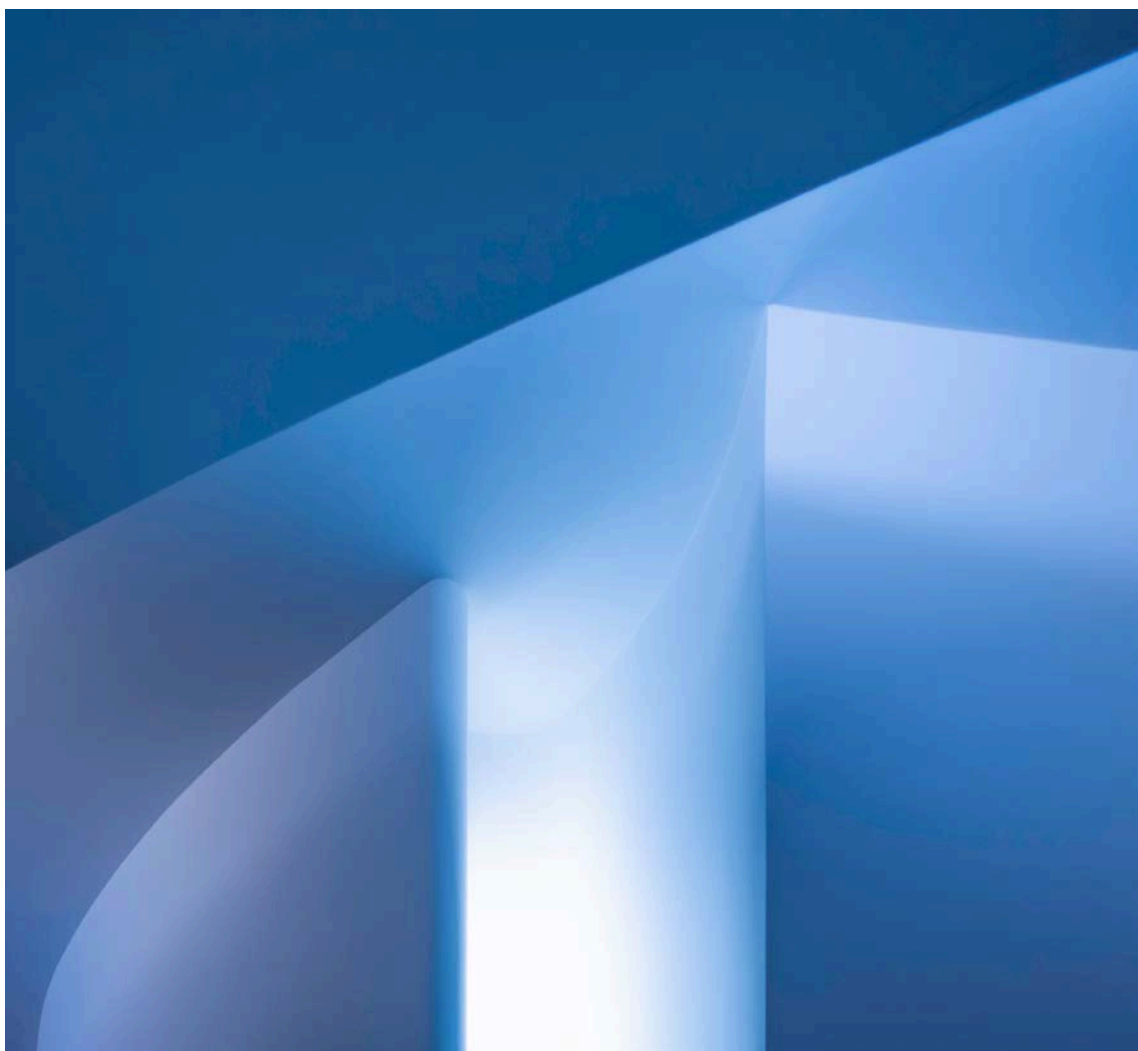
SECTION 003

重点国家知识产权诉讼方面的主要特点

从近年的案例中可以看出(如上页表所示),知识产权诉讼主要发生在美国、欧洲以及亚洲等重点国家,并呈现出各国独特的特点。

以美国为例,中国企业经常面临的知识产权相关争议主要包括商业秘密争议、专利诉讼争议(包括标准必要专利)、337调查、美国实体名单争议等。在涉及美国的某些案件中,不排除会启动司法部、FBI等刑事调查程序。以表中的美国超导与华锐风电的案件为例,案件包含了商业秘密的刑事犯罪、商业秘密侵权的民事程序、软件侵权的民事程序以及合同民事争议等,其中刑事调查涉及了美国、中国和奥地利三个国家,民事诉讼涉及中国、美国等多个法域。在美国的有关专利争议中,海外实体经常会采用专利诉讼和337调查相结合的策略(例如通领科技在美国经营过程中就不断受到竞争对手通过专利诉讼和337调查方式的包围)。美国的知识产权诉讼的特点主要包括证据开示制度、陪审团制度、马克曼听证等。作为英美法系的典型代表,如何灵活地利用美国诉讼程序和实体抗辩,是中国企业在美国市场上进行商业活动时需要关注的问题。

以欧洲为例,中国企业经常面临的知识产权相关争议除了传统的知识产权争议之外,还包括数据隐私争议(GDPR)、标准必要专利争议、海关/展会相关争议等。由于欧盟与各成员国之间在法律规定上有共同点又有各自独特之处,因此在面临知识产权争议时需要同时关注欧盟法律规定以及各成员国自身的法律规定。以专利为例,中国企业在欧洲参与展会活动时(例如西班牙MWC,德国IFA)经常会面临法院的临时禁令,如果应对不利,则会导致撤展的后果。而中国企业在进入欧洲市场时,也经常会碰到竞争对手或NPE利用专利诉讼的手段(包括临时禁令和永久禁令)谋取经济利益(典型的案例包括TCL vs 爱立信、TCL vs LG、海信vs



LG、海尔vs Sisvel、联想vs InterDigital、中兴vs Conversant等)。如何在诉讼发生之前(例如提交保护信)和诉讼发生之后进行有效的应对,是中国企业需要关注的难题。

亚洲新兴市场以印度为例,由于印度目前已经成为除中国之外最大的市场主体,因此全球的企业都试图在印度占有一席之地,这势必会产生激烈的市场竞争。作为压制竞争对手的重要手段,知识产权相关的诉讼争议必不可少(例如OPPO vs杜比案中,杜比公司就采用了临时禁令等多种手段向OPPO等公司提起诉讼)。印度由于沿袭了英国的大量制度,因此在司法体制上与英国有共通之处。以专利为例,专利权人可以向印度法院请求临时禁令和永久禁令,如何进行有效的应对是企业进行经营活动时需要考虑的重要因素。

SECTION 004

上市/拟上市公司面临境外知识产权诉讼时的应对策略

在知识产权诉讼风险较高的国家(例如美国、欧洲等)进行经营活动时,需要充分考虑到诉讼风险,并提前进行准备,并可以参考以下的应对策略。

(一)企业知识产权合规体系的建立

企业需要根据主要市场,就不同国家的法律体系建立相应的企业合规体系。以高科技类企业以欧美为主要市场为例,合规体系的重点包括研发法律合规体系、商业秘密风控管理体系、知识产权成果管理体系、IP预警和维权体系、合作伙伴风险管理体系等。

(二)企业重点知识产权风险评估

企业在进入知识产权诉讼风险较高的国家之前,需要进行知识产权方面的风险评估。知识产权方面的风险评估主要包括专利风险评估、商标风险评估、版权风险评估、数据隐私风险评估、商业秘密风险评估等。以专利风险评估为例,企业需要根据行业的特点和主要竞争对手的情况,提前了解重要的风险专利的布局情况和法律状态。在识别出高风险专利时,需要综合考虑谈判许可、规避设计、合同约定等各种方式来降低风险。如果穷尽各种手段仍然无法排除风险,则需要慎重考虑是否进入这些国家。

(三)企业诉讼策略评估

企业在进入知识产权诉讼风险较高的国家之后,需要持续关注市场的动态以及潜在的侵权风险。一旦发生诉讼争议,则需要对知识产权诉讼进行整体性评估。在难以胜诉并且对正常经营活动会产生较大影响的情况下,可以尝试谈判和解的方式来尽早解决争议。以专利诉讼为例,由于美国法院和ITC都较偏重保护专利权人的利益,因此在充分评估后认为胜诉较难或者不希望拖入持久战的情况下,双方和解也不失为企业最有利的解决诉讼争议的方式,且能尽可能地节省诉讼成本,并降低对上市公司可能造成的不利影响。当然,如果企业考虑积极应诉,则可以考虑充分利用各国的诉讼规则来尽可能争取胜诉。例如可以利用美国的PGR和IPR程序对专利的有效性提出挑战,利用欧洲的专利异议程序以

及各成员国法院的抗辩程序挑战专利的有效性。以TCL、海信、海尔、联想、中兴和OPPO在海外所面临的标准必要专利诉讼争议为例,由于诉讼相对方经常拥有大量的SEP专利,因此综合运用各种手段对专利的稳定性和对标与否提出挑战,可以在许可费率的谈判中变被动为主动,从而为最终解决双方争议争取筹码。

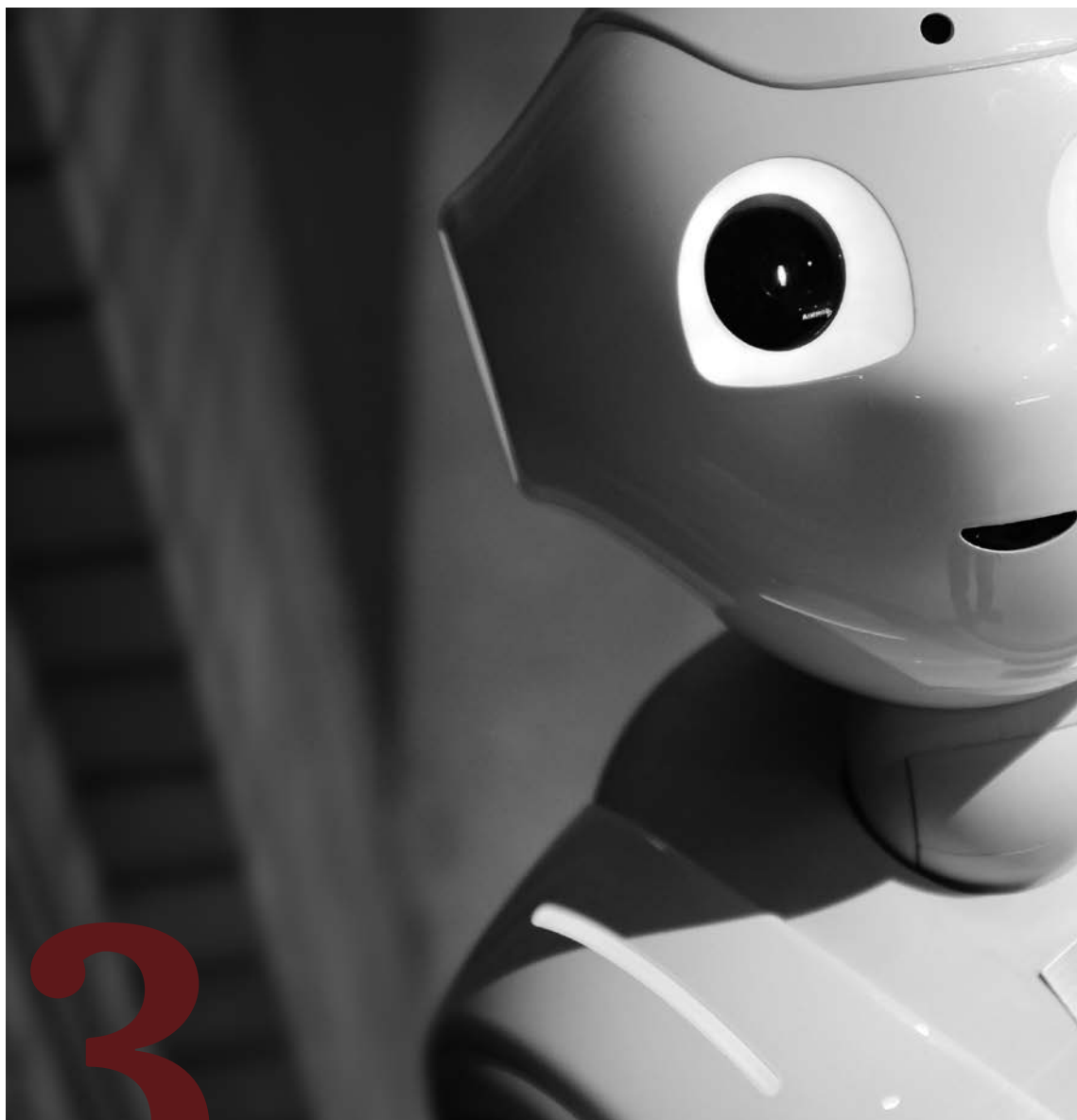
总之,上市/拟上市公司在进入海外市场时,需要根据不同国别建立起有效的知识产权合规体系,密切关注所在国家的司法动态和诉讼环境,在主动采取维权手段或者被动参与应诉活动时,需要综合考虑各种潜在风险和利弊,并且在必要时根据中国证券市场的监管规定及时披露重大诉讼事项,以降低对企业在本土市场上的经营活动的不利影响,并尽可能维持企业在海外市场上的竞争优势。



张诗伟/合伙人
资本市场部
北京办公室
+86 10 5957 2022
zhangshiwei@zhonglun.com



蔡鹏/合伙人
知识产权部
北京办公室
+86 10 5087 2786
caipeng@zhonglun.com



CHAPTER 03

企业进行人工智能技术开发 和技术保护路径探析

作者:蔡鹏/潘聪

人工智能技术作为底层的核心技术,对新基建中其他应用领域的实现起到了至关重要的支撑作用。本文从现实技术角度出发,讨论企业进行人工智能技术开发和保护的相关法律问题,浅析现阶段人工智能技术开发中所包含的法律风险,并进而对人工智能技术作为无形资产的保护方式和路径进行了初步的研判。

SECTION 001

人工智能的发展趋势和开发热点

1. 参见中国人工智能产业发展联盟AIIA《中国人工智能产业知识产权白皮书(2019)》，2019年12月

随着理论研究的突破和应用领域的拓宽,人工智能技术获得了较大的发展,目前主要包括芯片层、基础层、感知层、认知层和平台层这五个方面。

其中,芯片层是硬件基础;基础层包括人工智能基础算法、大数据技术、大计算技术;感知层包括语音技术和视觉技术以仿真人的听觉和视觉;认知层包括自然语言处理、推荐与搜索、决策与推理,并通过知识图谱、语义理解、机器翻译等方面实现大规模产业化应用;平台层作为接口将人工智能能力进行输出,从而助力各行业领域智能化升级¹。因此,人工智能技术已经形成完备的从芯片层到平台层的生态体系,在各层内的理论研究和应用开发如火如荼,相对而言,底层技术的每次创新突破都会带来上层应用技术的百花齐放。

目前在芯片层,为特定应用场景定制的芯片技术研究是当前的开发热点,孕育了寒武纪、地平线这样的独角兽企业。在基础层方面,机器学习、神经网络、5G边缘计算、量子计算、大数据存储、计算、分析与挖掘都是研究人员关注的相关热点。对于感知层而言,语音识别和合成、计算机视觉都是为实现机器能听能看的研究重点。在认知层方面,对话系统、机器翻译、语义分析和理解、知识图谱是为提升人机交互能力的技术热点。最后在平台层上,研究人员更多的是关注如何将底层的人工智能技术应用到金融、医疗、安防、交通、教育、工农业、通信、物流、智能家居等各行各业中,以期赋能各行业的智能化升级¹。

SECTION 002

人工智能知识产权保护的现状

目前人工智能技术的知识产权保护主要涉及专利、技术秘密、软件著作权这三个方面,对于这三种保护方式的优劣,本文简要归纳如下表所示。

项目	专利	技术秘密	软件著作权
保护期	发明专利20年	长期	根据开发主体而定
保护内容	人工智能应用的技术方案	人工智能算法、源代码、数据以及know-how等不能公开的有价值的内容	计算机程序整体
商业模式	专利期内的垄断权, 专利转让/许可/运营/质押/投融资	利用技术秘密取得产品的竞争优势	软件著作权许可/转让
诉讼优势	利用专利获得禁令救济、诉讼赔偿等	利用版权/反不正当竞争获得禁令救济、诉讼赔偿等	利用版权诉讼获得禁令救济、诉讼赔偿等
诉讼风险	取决于专利本身的撰写质量, 或者专利被无效的风险	现有诉讼制度下, 较难举证侵权产品是否采用相同/类似代码或技术	举证难度大
保护局限	专利保护侧重人工智能应用, 而非人工智能算法本身, 因此纯人工智能算法较难获得专利权	存在泄密风险, 需要严格且有效的保密措施	可能受开源协议的约束; 存在第三方利用专利/版权维权的可能性

从上表中可以看出, 企业通过专利、技术秘密、软件著作权这三种途径来保护人工智能技术各有利弊, 下面本文从这三个方面进行详细介绍。

2.1 专利保护

国家知识产权局于2019年12月31日专门修订了《专利审查指南》, 以回应创新主体对进一步明确涉及人工智能等新业态新领域专利申请审查规则的需求, 修订后的指南已于2020年2月1日起开始施行。

修订后《专利审查指南》在第二部分第九章中增加第6节, 其中在审查基准中提到以下标准:

1. 审查应当针对要求保护的解决方案, 即权利要求所限定的解决方案进行。在审查中, 不应当简单割裂技术特征与算法特征或商业规则和方法特征等, 而应将权利要求记载的所有内容作为一个整体, 对其中涉及的技术手段、解决的技术问题和获得的技术效果进行分析;

2. 如果权利要求中除了算法特征或商业规则和方法特征, 还包含技术特征, 该权利要求就整体而言并不是一种智力活动的规则和方法, 则不应当依据专利法第二十五条第一款第(二)项排除其获得专利权的可能性;

3.对一项包含算法特征或商业规则和方法特征的权利要求是否属于技术方案进行审查时,需要整体考虑权利要求中记载的全部特征。如果该项权利要求记载了对要解决的技术问题采用了利用自然规律的技术手段,并且由此获得符合自然规律的技术效果,则该权利要求限定的解决方案属于专利法第二条第二款所述的技术方案。

由此可见,相对于以往专利审查中针对算法类发明和商业方法类发明的审查标准,较严格而难以获得授权、并且实质审查中往往存在审查标准不一致的问题,目前对于人工智能技术的专利保护,国家知识产权局已经对审查标准予以明确的规范,并为专利申请人指明了方向。也即,专利申请人需要将人工智能技术应用于相应的技术领域,以采用技术手段来解决技术问题,并实现相应的技术效果,这样才有可能获得专利权的垄断保护,否则可能存在客体问题而无法授权。

目前来看,虽然利用专利保护人工智能技术能够获得有限期限内绝对的垄断优势,并且可以利用专利运营获得资金来源,在被侵权时也可以利用专利诉讼来合理维权,但是,采用专利权保护人工智能技术有以下弊端:第一,只能获得有限期(发明专利20年)的保护期限;第二,只能保护能够应用于具体技术领域的人工智能技术方案,无法覆盖全部的人工智能技术研究场景;第三,在举证方面,如果人工智能技术偏底层而非表现应用,则存在举证难度大的困境。

2.2 技术秘密保护

根据《反不正当竞争法》的规定,商业秘密是不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。在人工智能产品开发场景下,基础算法、结构化数据等信息均为企业花费大量的人力物力投入所获取,且不易/不便采用专利方式进行保护的客体,此时采取商业秘密保护是合适的保护方式。

我国商业秘密保护的法律制度近年来有诸多变化,主要如下:

- 1.随着《反不正当竞争法》的修订和2020年1月《中华人民共和国政府和美利坚合众国政府经济贸易协议》的签署,商业秘密案件的举证责任将会有较大变化,权利人举证难的情况会有所改观。可以预见的是,权利人需要证明“接触+初步证据”,法院可能将举证责任转移至被告。但如何界定“初步证据”,还有待于有关司法实践予以阐明。

- 2.修改后的《反不正当竞争法》不仅大幅调高了法定赔偿,还增加了惩罚性赔偿制度,即经营者恶意实施侵犯商业秘密行为,情节严重的,赔

偿数额可能加倍(一至五倍)。有的地方法院系统在司法文件中已经对适用惩罚性赔偿中的关键条件“恶意”进行了界定,明确了惩罚性赔偿的适用原则。但如何运用到具体案件中,特别是法院如何将法定赔偿、裁量性赔偿与惩罚性赔偿进行结合,有效弥补权利人损失,还尚需观察。

3.对经营者侵犯商业秘密的行为进行了相应的扩充,其中增加了“以电子侵入获取权利人的商业秘密”、“违反保密义务,披露、使用或者允许他人使用其所掌握的商业秘密”、以及“教唆、引诱、帮助他人违反保密义务或者违反权利人有关保守商业秘密的要求,获取、披露、使用或者允许他人使用权利人的商业秘密。经营者以外的其他自然人、法人和非法人组织实施前款所列违法行为的,视为侵犯商业秘密”等相关内容。

虽然采用商业秘密方式来保护人工智能技术可以获得无期限的保护,但是也存在以下弊端:

第一,人工智能技术是目前经济社会的研究热点和各国争夺的科研高地,研发人员的流动性较高,被网络窃取攻击的行为也并不鲜见,因此采用商业秘密/技术秘密保护人工智能技术势必存在非常高的泄密风险。

第二,法律制度尚待完善,泄密之后维权收益与损失差距明显。商业秘密的特点即“一旦失去将永远失去”,商业秘密的公开或不当泄露会给权利人带来无法估量的损失。特别是人工智能领域竞争相当激烈,员工跳槽、竞争对手挖角等行为导致商业秘密流失的情况并不鲜见,现有法律赔偿机制下仍无法剿灭或有效限制此种不法行为所带来的可期待非法收益。

2.3 软件著作权保护

计算机软件是法定的著作权保护客体,但是计算机软件保护受限于著作权“思想表达二分法”,在多层的人工智能技术体系中,位于底层的基础技术难以获得并进行比对,而位于表层的各项代码却容易通过修改语言以达到区分表达的效果。因此,人工智能企业在对核心技术和软件进行保护时,还是倾向于采取专利和商业秘密的方式。

另一个难以回避的问题就是开源软件对软件著作权的影响,这是由于人工智能技术研发的难度不断增大、企业在科研投入上存在成本压力,因此目前互联网行业的很多企业纷纷采用开源的方式来进行人工智能技术的推进和研发。以谷歌、微软、Facebook为例,这些企业除了维护自己的某些开源项目之外,还分别在影响力较大的项目托管平台(例如

Github) 上开源大量的项目, 以供全世界的开发者集思广益, 从而推动项目的研发和落地。

采用开源的方式公开企业自身的研发成果看似无利可图, 但实际上企业在开源后不仅可以促进技术项目的研发, 还可以通过各种商业变现方式来支持企业发展, 比如企业可以通过双重授权 (例如向客户销售性能更好的企业版本)、提供增值业务 (例如谷歌在Android底层基础上提供GMS增值业务)、提供技术维护/服务 (例如Redhat为企业提供相应的订阅维护服务)、提供广告 (例如Mozilla提供广告服务) 等方式来获得资金收入。

但是, 企业在使用开源代码的过程中, 如果不注意开源协议的遵守, 可能会受到开源代码贡献者利用版权/专利权进行诉讼的风险。而企业在主动将内部的技术/代码开源的同时, 势必也会招致某些第三方 (如NPE) 诉讼维权的风险, 例如第三方可以采用版权/专利权的方式来进行侵权诉讼 (如甲骨文vs谷歌)。此外, 在企业主动开源之后, 如果使用企业开源代码的用户并未遵守开源协议, 也势必会引起商业或诉讼纠纷, 此时企业可能需要拿起版权/专利权的武器来压制对手, 否则可能会存在失去商业竞争优势的风险。

SECTION 003

企业保护人工智能技术的途径

考虑到人工智能技术采用专利、技术秘密、软件著作权等方式进行保护各有利弊, 企业需要根据实际场景/产品的不同情况综合权衡, 从而做出最有利的抉择, 下文给出企业在选择采用何种途径进行保护时需要注意的关注点。

3.1 利用专利保护人工智能技术的注意事项

企业在考虑利用专利权进行人工智能技术的保护时, 需要从以下两个方面去考虑可行性和相关风险:

1) 哪些技术适合专利权的保护。如果是纯算法的理论研究, 可能较难获得专利保护; 而如果这些算法能够应用于某些技术领域来解决相应的技术问题, 并且竞争对手容易模仿或者通过反向工程来获得这些技术, 则建议采用专利权进行人工智能技术的保护。

对于人工智能技术专利保护的主体, 企业至少需要考虑技术的重要



企业在吸引优秀人才加盟的同时,还需要做好内部风险的隔离机制,避免在不知情或未授权的情况下利用到第三方的技术秘密,从而造成被起诉调查的不利局面。

性和维权的便利性这两个维度。如果某项人工智能技术对企业来说至关重要,并且企业决定采用专利方式进行保护,则需要聘请专业的机构来进行全方位的布局,以避免由于撰写失误导致客体的问题、或者由于专利布局不周而无法进行有效保护。另外,考虑到维权的便利性,企业应当将容易举证的体现表现功能或应用场景的创新技术通过专利方式进行保护,以创新产品新模式/新样态(例如某两电子科技公司知识产权案中涉案专利“组件显示处理方法和用户设备”)。

2) 专利申请“危险期”的问题。专利的申请日对于判断专利申请的新颖性和创造性具有重要的作用,而对于人工智能企业而言,企业专利的数量和质量也是决定其企业价值和竞争力的重要指标,故企业很容易忽视人才在流转过程中专利申请的“危险期”。根据《专利法实施细则》12条的规定,退休、调离原单位后或者劳动、人事关系终止后1年内作出的,与其在原单位承担的本职工作或者原单位分配的任务有关的发明创造为职务发明创造。由于职务发明创造归属于原单位,因此离职1年~2年期内都属于“危险期”。

需要特别注意的是,1年内为作出发明创造的时间,并非专利的申请时间。只要是离职员工在离职1年内作出的,即使在1年后才进行专利申请,应该同样为职务发明创造。因此,企业不仅要关注专利申请时间,更要关注发明创造的完成时间。在(2004)沪二中民五(知)初字第117号案中,原告公司与被告史某于1998年6月订立劳动合同,2001年2月28日被告从原告公司辞职,并于2002年12月23日申请了涉案专利。法院认为本案关键在于需要查明被告以个人名义申请的涉案专利是其在原告任职期间执行单位任务开发完成的,还是其离职后依靠个人能力开发完成的。经过技术鉴定,被告在离职1年后作出的发明创造与其在原告处完成的发明创造完全相同,该发明创造应属于被告执行原告单位的课题研究任务,在本职工作中所完成的发明创造。因此法院判决专利权归公司所有。

3.2 利用商业秘密保护人工智能技术的注意事项

企业在考虑利用商业秘密进行人工智能技术的保护时,需要从以下几个方面去重点关注:

1) 企业保密体系的有效建立和实施。对有关技术采取合适的措施进行保护是维护商业秘密的第一步,没有适当的保密措施将会直接影响法定商业秘密的成立。考虑到人工智能技术的开发特点,会涉及算法开发、数据开发等若干关键岗位,因此企业需要制定完善的内部管理规范,如

保密制度、保密手册、网络安全规章、数据保护制度、网络安全应急响应机制、员工保密协议、员工竞业禁止协议、项目隔离机制、项目研发流程规范、代码接触审批机制等。企业应当避免对公司全员采用同一版本的保密协议,而应将有关的保密义务和法律责任对应到关键技术研发人员,同时也要有相应的研发奖励制度,做到奖惩一致。企业在实施保密体系过程中,要根据不同阶段对团队和研发情况进行调整,既要保证核心机密文件不因员工的流失而泄露,也要确保追责的有效和证据的可回溯性。

2)做好风险隔离机制。人工智能行业人才的高流动性容易导致研发风险的产生。企业在吸引优秀人才加盟的同时,还需要做好内部风险的隔离机制,避免在不知情或未授权的情况下利用到第三方的技术秘密,从而造成被起诉调查的不利局面。在核心技术人员引进的过程中,人工智能企业应当与其订立有关的技术隔离和法律隔离文件,明确其知晓公司的相关规章制度,确保其没有带入或在职务中使用前雇主的涉密资料,消除技术资料被滥用的风险。

3)完善物理层面的安全控制。企业可以通过自建/购买网络防火墙、加解密技术、网络/数据监控技术来为企业构建尽可能安全的网络安全体系。一是防止外来技术侵入和窃取,二是做好资料备份存储,防范内部员工不当下载和泄露。另外,在发生网络被攻击或者泄密事件时,企业需要能够及时响应,从而尽可能降低泄密风险,避免对企业的正常运营造成损失。

3.3 软件开源对人工智能技术保护的影响

如果企业基于研发或商业的考虑,选择对人工智能技术进行开源,则需要考虑开源平台的选择、开源协议的选择、内部开源制度的构建等各方面。虽然企业对人工智能技术软件/代码进行开源,但实际上企业仍然享有软件著作权/版权,通常来说只是将版权免费授权给用户使用,在用户违反开源协议的情况下,企业有权利利用版权等方式合理维权。

在开源平台方面,企业可以选择自己构建、或者利用现有的平台(例如Github、Gitlab、coding、码云等)来实现。自建的优势在于能够自主做决策,并对项目的运行有较大影响力。但自建的成本较高,需要考虑购置相应的设备、安排人手对开源社区进行主动维护、信息泄露对开发者造成的影响等各种因素。利用现有平台可以节省成本,但由于受制于人,因此也存在不可控的因素。而且,如果项目的影响力不够,则可能并不能达

到项目的预期。需要注意的是,企业需要特别关注内部员工/前员工泄露公司代码的风险(如某视频网站、某创新科技公司等代码泄露案),在这方面,企业可以通过在开源平台上进行日常的搜索和巡检来规避这样的风险。目前常用的开源平台简要归纳如下表所示。

项目	Github	Coding	码云
平台影响	全球	中国	中国
出口管制	适用美国EAR	未提及	未提及
关联方	微软收购	腾讯投资	百度投资
免责条款	IP等责任免责	IP等责任免责	IP等责任免责
无担保责任	有	有	有
泄密风险	较大	中等	中等

在开源协议方面,企业需要根据自身的商业模式来选择最优的开源协议。目前常用的开源协议包括GPL、MPL、BSD、MIT和apache等,其中GPL和MPL协议的衍生代码存在无法商用的风险,但适合决定采用双重授权或硬件绑定方式进行商业运营的企业(例如IBM通过绑定免费的Linux来获得硬件销售优势)。而BSD、MIT和apache代码虽然较为宽松,但由于BSD和MIT协议并未约定专利权等授权条款,因此理论上可能存在被代码开源者/贡献者利用专利诉讼等方式进行维权的风险。目前常用的开源协议简要归纳如下表所示。

项目	能否闭源	商标授权	版权授权	专利授权	法律文本
GPL	不能	无	有	有	英文
MPL	不能	无	有	有	英文
BSD	能	未提及	有	未提及	英文
MIT	能	未提及	有	未提及	英文
apache	能	无	有	有	英文
木兰许可证	能	无	有	有	中英文

在内部开源制度的构建方面,为了避免代码开源的风险,建议企业建立内部开源项目/开源代码的审查制度,不仅需要对企业利用的开源代码风险进行法律评估,还应当对企业自有项目/代码是否适宜开源进行评估,从而尽可能降低企业整体运营风险。

SECTION 004

小结

总体而言,在现实技术发展下,企业对人工智能技术的保护倾向于采取专利+商业秘密的保护策略,对人工智能技术的开发越来越多采用“去中心化”式的研究策略,以构建共享和收益的技术生态圈。具体从保护竞争优势的角度来看,企业需要结合自身人工智能技术的特征来选择相对应的保护方式,从而构建多方位、多角度的立体保护格局,以规避法律风险,达到最优化的商业目标。



蔡鹏/合伙人
知识产权部
北京办公室
+86 10 5087 2786
caipeng@zhonglun.com

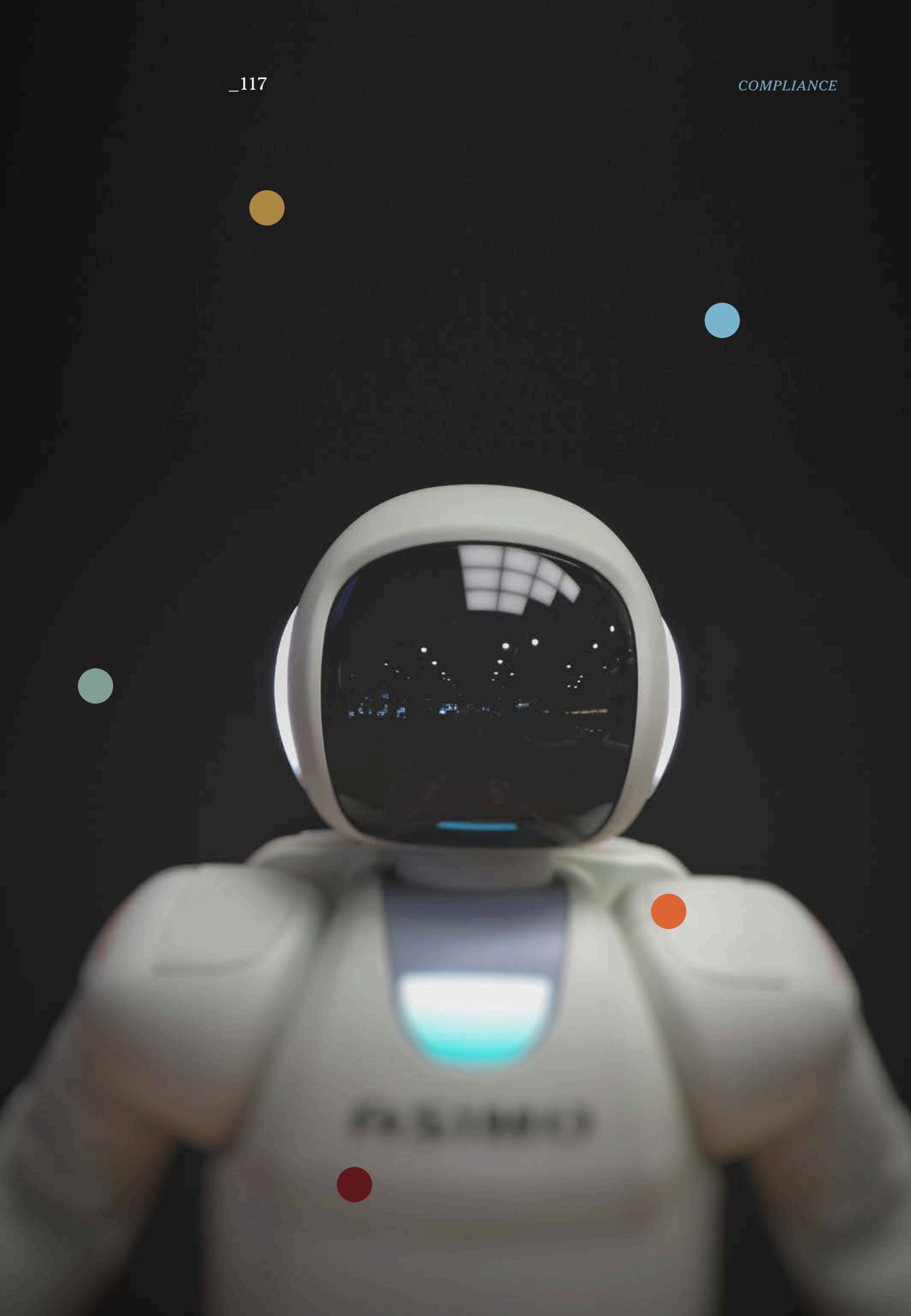
CHAPTER
FOUR

COMPLIANCE

肆

合规运营篇

CHAPTER FOUR





1

CHAPTER 04

科技企业上市 之数据合规

作者:陈际红/韩璐/王雨婷

数据是现代企业的血液,以大数据或互联网为工具开发新型服务或产品的传统行业企业也依赖数据带来新的业务增长点。随着《中华人民共和国网络安全法》(“《**网络安全法**》”)正式生效并逐步深入落实,网络安全执法活动日趋活跃,科技企业的网络安全及数据保护合规状态亦成为监管机关的重点关注内容。

对于科技企业上市而言,数据不仅作为企业资产价值评估的重点,其全流程管理的合规现状也已成为上市审核的核心要素。从数据堂员工涉嫌刑事犯罪到墨迹天气上市申请被否,在《网络安全法》生效的不到三年内,数据合规问题逐渐从幕后走向台前,走入大众视野,也落入上市审核机关的“射程”范围内。拟上市企业、保荐机构、会计师事务所与律师事务所若只关注企业盈利能力、关联交易、应收账款,而忽视了企业对数据的管理,数据合规问题则可能成为拟上市企业的阿克琉斯之踵。在数据收集、数据融合、数据的二次开发、数据流转、用户推送等环节稍有不慎,数据合规问题可能成为企业上市的“拦路虎”,甚至引发刑事责任:

--2017年8月11日,数据堂(北京)科技股份有限公司因员工涉嫌侵犯公民个人信息罪而作出公司股票暂停转让的公告。¹

--2018年4月4日,中国证券监督管理委员会(“证监会”)第十七届发行审核委员会(“发审委”)2018年第57次发审委会议审核北京博睿宏远数据科技股份有限公司²(创业板)(首发)未通过。

--2018年11月2日,北京瑞智华胜科技股份有限公司因涉及特大数据泄露案件于新三板终止挂牌。2019年10月28日,越城区人民法院宣判北京瑞智华胜科技股份有限公司犯非法获取计算机信息系统数据罪,判处有期徒刑人民币10,000,000元,公司法定代表人及涉案员工共七人分别被判处2年至3年6个月不等刑期,并处罚金。

--2019年3月5日,从事互联网数据服务的天聚地合(苏州)数据股份有限公司创业板上市申请终止审查。

--2019年10月11日,发审委审核北京墨迹风云科技股份有限公司(创业板)(首发)未通过。

1.《数据堂(北京)科技股份有限公司重大事项暂停转让公告》,2017年8月11日。

2.公司的主要业务主动式检测的实施需要在APP或服务器安装SDK及探针。

PART I 审核要点篇

为了协助科技企业在申请上市过程落实数据合规工作,妥善回应发审委问询,降低拟上市企业潜在的数据合规风险,我们梳理了自《网络安全法》生效以来审核机关对主板、创业板、科创板上市(或拟上市)企业、新三板挂牌企业及上市重组的审核问询,涉及共27家企业数据收集、数据权属、数据使用和共享、第三方处理、数据安全、数据立法和监管对业务的影响等涵盖企业整个数据生命周期的问题。同时,我们对上市过程

中审核机关关注的合规风险点进行了系统梳理并提出了相应合规建议,希望对拟上市科技企业开展数据合规工作提供帮助。

SECTION 001

企业上市面临的数据合规挑战

基于我们对公开材料的梳理,分别有1家主板上市企业、12家创业板上市(或拟上市)企业、9家科创板上市(或拟上市)企业、2家新三板挂牌企业(包括1家已停牌企业)在申请上市或挂牌过程中接受了发审委或交易平台关于数据合规问题的问询。此外,3家创业板上市企业在开展并购重组项目中,也因标的公司的数据相关业务接受了证监会上市公司并购重组审核委员会的问询。我们基于上述27家企业的招股说明书、审查反馈意见、问询函、发审委会议审核公告等文件,汇总整理了发审委重点关注的九类数据合规问题:数据源合规、数据权属、数据使用、数据共享、第三方处理、数据安全、系统与技术和数据立法和监管、数据相关的业务经营。

	创业板													上市重组					
	品牌管理	尚品宅配	科锐国际	深信服	博睿宏远*	每日互动	第三方支付#	值得买	宇瞳光学	壹网壹创	指南针	墨迹风云*	创业板问题统计	旗天科技	华铭智能	数知科技	上市重组问题统计		
数据源合规	1	1				6	1	1		1	2	1	14	22.6%			1	1	16.7%
数据权属						1							1	1.6%		1		1	16.7%
数据使用			1		1	7	1	1		1		2	14	22.6%		1	1	2	33.3%
数据共享						2							2	3.2%				0	0.0%
第三方处理													0	0.0%				0	0.0%
数据安全			1	3		5		2	1		1	1	14	22.6%		1		1	16.7%
系统与技术和数据立法和监管					1	2		1			1		5	8.1%				0	0.0%
数据相关的业务经营						3	2					2	7	11.3%		1		1	16.7%
	1	1	2	3	5	28	2	5	1	2	4	8	62		1	3	2	6	

* 为首发未通过、在审或停止挂牌企业

为匿名企业,以其所属行业或核心产品代称

	科创板										主板	新三板		总计		
	安博通	智能终端#	安恒信息	办公软件#	普元信息	优刻得	汽车智能诊断#	罗克佳华*	慧辰资道*	科创板问题统计	长沙银行	数据堂	瑞智华胜*			
数据源合规				1			3	1	3	8	25.0%			1	24	23.1%
数据权属									1	1	3.1%				3	2.9%
数据使用		1			1				3	5	15.6%				21	20.2%
数据共享									1	1	3.1%				3	2.9%
第三方处理					2					2	6.3%				2	1.9%
数据安全	2		2			3			3	10	31.3%				25	24.0%
系统与amp;技术										0	0.0%	1			6	5.8%
数据立法和监管									1	1	3.1%				6	5.8%
数据相关的业务经营					2				2	4	12.5%		1	1	14	13.5%
	2	1	2	1	5	3	3	1	14	32		1	1	2	104	

* 为首发未通过、在审或停止挂牌企业 # 为匿名企业，以其所属行业或核心产品代称

SECTION 002

企业上市须应对的数据合规重点问题

通过上述梳理，我们发现在创业板及科创板上市申报过程中，审核机关最关注的三类问题为数据源合规、数据安全及数据使用合规。这三类问题无疑应是拟上市企业数据合规治理的重中之重。在此，我们对百余个数据合规问题进行了梳理，以期全面展现拟上市企业将面临的数据合规问询。

3.《浙江每日互动网络科技股份有限公司创业板首次公开发行股票申请文件反馈意见》。

4.《中国证监会行政许可项目审查二次反馈意见通知书》；《关于请做好浙江每日互动网络科技股份有限公司发审委会议准备工作的函》。

5.《关于北京慧辰资道资讯股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函》。

6.《北京市万商天勤律师事务所关于公司首次公开发行人民币普通股(A股)股票并在创业板上市的补充法律意见书(四)》，口头反馈问题一(浙江每日互动网络科技股份有限公司)。

7.《关于对上海华铭智能终端设备股份有限公司的重组问询函》。

8.《中国证监会行政许可项目审查二次反馈意见通知书》；《北京市万商天勤律师事务所关于公司首次公开发行人民币普通股(A股)股票并在创业板上市的补充法律意见书(四)》，口头反馈问题一；《关于请做好浙江每日互动网络科技股份有限公司发审委会议准备工作的函》。

类别	问题
数据源合规	主要产品的研发周期、渠道推广和用户积累的过程，是否存在向第三方购买底层数据并在外购数据的基础上持续开发等情况。 ³
	获取用户数据信息的来源、获取途径及授权方式，收集用户信息获得用户同意的具体制度及相关安排，收集用户信息时是否明确告知收集信息的范围及使用用途。 ⁴
	对于公司向数据供应商购买数据的，请说明供应商授权公司使用相关数据是否经过终端用户或者其他第三方同意，授权是否完备合规，个人信息获取是否合法。公司是否建立完善的供应商评价体系，以及供应商甄选、数据源核验以及合同合规性审核的内控措施。 ⁵
	请发行人补充说明“个推大数据平台”的数据来源及合规性，包括数据的具体来源及协议。 ⁶
数据权属	标的公司采购所涉相关数据信息的产权归属及其法律依据。 ⁷
数据使用	获取数据进行商业化变现的合规性。 ⁸
	发行人通过 APP 授权获取的用户信息用于互联网营销或其他业务是否超过用户

9.《北京市万商天勤律师事务所关于公司首次公开发行人民币普通股(A股)股票并在创业板上市的补充法律意见书(四)》,口头反馈问题四(浙江每日互动网络科技有限公司)。

10.《中国证监会行政许可项目审查二次反馈意见通知书》;《关于做好浙江每日互动网络科技有限公司发审委会议准备工作的函》。

11.《北京墨迹风云科技股份有限公司创业板首次公开发行股票申请文件反馈意见》。

12.《关于普元信息技术股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

13.《关于北京慧辰资道资讯股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函》。

14.《关于北京慧辰资道资讯股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函》。

15.《关于对北京梅泰诺通信技术股份有限公司的重组问询函》(现名为北京数知科技股份有限公司)。

16.《关于做好浙江每日互动网络科技有限公司发审委会议准备工作的函》。

17.《关于北京慧辰资道资讯股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函》。

18.《关于普元信息技术股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

19.《关于普元信息技术股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

20.《关于做好相关项目发审委会议准备工作的函》(北京科锐国际人力资源股份有限公司)。

21.《关于做好发审会议准备工作的函》(深信服科技股份有限公司)。

类别	问题
数据使用	对 APP 的授权范围。 ⁹
	对数据的使用是否超过必要的限度。 ¹⁰
	发行人运用大数据相关技术从事精准推荐和个性化营销服务是否涉及侵犯产品用户个人隐私或其他侵权风险,发行人的大数据相关技术及其使用、相关服务的开展的合法合规性,是否存在纠纷或潜在纠纷。 ¹¹
	发行人是否有权接触、保管、处理相关数据,是否需取得最终个人的授权许可。 ¹²
	发行人收集、整合、处理、使用数据是否符合《数据安全管理办法》的规定,是否制定并公开收集使用规则,是否向所在地网信部门备案,是否存在违反收集使用规则使用个人信息的情况。 ¹³
	发行人使用用户数据是否合法合规,请对照《网络安全法》、《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》、《信息安全技术个人信息安全规范》等法规和司法解释,说明报告期发行人是否存在侵犯用户隐私或数据的情况,是否存在法律风险或潜在法律风险。 ¹⁴
数据共享	请补充说明标的公司对用户信息的收集、传输、保存及应用的现状是否符合2018年5月1日实施的《信息安全技术个人信息安全规范》的要求。若否,请充分提示相关风险并说明后续整改措施。 ¹⁵
	抽样头部 APP 产品的《用户协议》、《隐私政策》中部分表述基于提升本 APP 服务之目的而收集用户数据并向第三方共享该数据,发行人链路共享是否属于“提升本 APP 服务之目的”。 ¹⁶
第三方处理	发行人的数据是否存在转授权或流转给第三方使用的情况,如存在,是否经过了个人信息主体的明示同意,是否经过了充分的脱敏,相关授权流程是否完备。 ¹⁷
	各个下游行业对第三方进行数据处理方面的相关政策。 ¹⁸
数据安全	相关业务的开展方式及相关数据的使用方式,行业是否允许第三方机构处理相关数据,是否需取得有权主管部门批准。 ¹⁹
	对相关信息是否存在有效的保密机制,是否符合《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国网络安全法》的规定。 ²⁰
	说明在开展业务、日常运营过程中是否获取或有可能获取国家秘密、保密信息、个人信息,是否存在泄漏国家秘密、保密信息、个人信息的情况或未来风险,是否已建立完善的防泄密和保障网络安全的内部管理制度,该等制度的执行是否有效。 ²¹
	说明是否需要进行信息安全等级保护测评。 ²²
	最近三年发生的严重泄密事件、重大诉讼、处理结果及有关的整改措施。 ²³
	公司主要客户为政府、金融部门、公安部门、医疗等部门,在为客户提供云平台、大数据存储等服务中可能涉及国家或地方政府政治、经济、金融、卫生、安全等领域涉密信息。请发行人对自身业务层面潜在的或可能面临的数据或信息被窃取、篡改、泄露、假冒、恶意破坏或被攻击等网络安全事件风险和法律风险及应对措施或解决方案向投资者进行充分提示。 ²⁴
	数据安全相关制度及措施,包括但不限于数据的备份机制、防范数据窃取及泄露的措施、对用户隐私数据加密措施以及对于到期数据的处理机制等。 ²⁵

类别	问题
系统与amp;技术	用户信息保护技术体系,尤其是防止外部黑客攻击和内部人员恶意导致的数据泄露的技术措施。 ²⁶
	说明运营系统和财务系统的数据是否衔接,IT审计是否实施到位。 ²⁷
	招股说明书披露,发行人的核心技术主要体现在移动客户端技术、大规模通信技术、分布式处理技术、广告计算技术、大数据技术以及大规模数据存贮技术等。补充披露发行人主要技术、核心技术的来源、形成过程及合法合规性。 ²⁸
数据立法和amp;监督	欧盟《通用数据保护法案》(General Data Protection Regulation, GDPR)的颁布实施对于发行人经营业务有什么影响,发行人有什么整改措施,是否存在被处罚的风险,GDPR对于发行人未来的业务经营是否存在影响。 ²⁹
	主管部门对数据隐私保护的标准是否会持续升级,未来的趋势对业务的影响及相关应对措施。请说明发行人在数据保护及个人隐私安全等方面是否符合相关规定。 ³⁰
	发行人针对APP专项治理工作组通知指出问题的整改情况及整改效果,是否获得主管部门的认可,是否面临被处罚的风险。 ³¹
数据相关的amp;业务经营	披露标的公司业务模式是否存在侵犯消费者知情权、公平交易权、个人信息安全权的情形。 ³²
	说明发行人进行主动监测业务是否涉及对客户APP及服务器的信息数据使用,是否需经过客户许可或网站、APP的使用授权,是否涉及对网站、APP具体使用者商业秘密、个人隐私的侵犯;以上涉及授权的是否已合法合规签订使用授权协议或完成其他形式的授权;是否导致诉讼或潜在法律风险。 ³³
	在大数据业务、云计算中具体提供的软件名称和业务范围。 ³⁴
	与客户所签署业务合同的业务范围条款和保密条款是否存在协助或变相协助客户、第三方开展可能侵犯第三方商业秘密或个人信息安全的行为。 ³⁵
	与客户签订的服务协议中对于潜在安全泄露的责任约定与免责条款。 ³⁶
	公司业务中是否涉及用户的隐私数据,问询回复中认定“不曾亦不会获取用户的隐私数据”的依据是否充分合理。 ³⁷
	请发行人针对数据获取途径说明各类途经的具体内容、标准及占比,发行人是否掌握核心数据来源,此种运营模式是否与同行业可比公司相同或相似,是否存在数据来源的风险,是否对数据供应商存在重大依赖。 ³⁸

22.《关于做好发审会议准备工作的函》(深信服科技股份有限公司)。

23.《中国证监会行政许可项目审查二次反馈意见通知书》;《关于做好浙江每日互动网络科技股份有限公司发审会议准备工作的函》。

24.《关于杭州安恒信息技术股份有限公司首次公开发行股票并在科创板上市申请文件的第二轮审核问询函》。

25.《关于优刻得科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

26.《中国证监会行政许可项目审查二次反馈意见通知书》;《关于做好浙江每日互动网络科技股份有限公司发审会议准备工作的函》。

27.第十七届发审委2018年第57次会议审核结果公告,北京博睿宏远数据科技股份有限公司(首发)未通过。

28.《浙江每日互动网络科技股份有限公司创业板首次公开发行股票申请文件反馈意见》。

29.《北京市万商天勤律师事务所关于公司首次公开发行人民币普通股(A股)股票并在创业板上市的补充法律意见书(四)》;《口头反馈问题三》;《中国证监会行政许可项目审查二次反馈意见通知书》;《关于做好浙江每日互动网络科技股份有限公司发审会议准备工作的函》。

30.《中国证监会行政许可项目审查二次反馈意见通知书》(浙江每日互动网络科技股份有限公司)。

31.第十八届发审委2019年第142次会议审核结果公告,北京墨迹风云科技股份有限公司(首发)未通过

32.并购重组委2016年第47次会议审核结果公告,上海康耐特光学股份有限公司发行股份购买资产方案审核意见(现名为旗天科技集团股份有限公司)。

企业在创业板与科创板申请上市过程中涉及的上述数据合规的问询问题覆盖了企业数据全生命周期的管理活动。除此之外,我们观察到主板上市企业也在申请上市过程中被要求说明其系统是否安全稳定可靠,是否开展了IT审计,以及如何确保数据获取的可靠性与准确性。上市企业推进数据业务相关的并购重组项目时也会面临并购重组审核委员会对标的公司提出的类似问询,这对于拟上市企业也具备一定的参考价值。

同时,新三板挂牌企业同样面临数据合规问询以及数据合规风险,甚

33.《北京博睿宏远数据科技股份有限公司创业板首次公开发行股票申请文件反馈意见》。

34.《关于普元信息技术股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

35.第十七届发审委2018年第57次会议审核结果公告,北京博睿宏远数据科技股份有限公司(首发)未通过。

36.《关于优刻得科技股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

37.《关于北京慧辰资道资讯股份有限公司首次公开发行股票并在科创板上市申请文件的第三轮审核问询函》。

38.《关于北京慧辰资道资讯股份有限公司首次公开发行股票并在科创板上市申请文件的审核问询函》。

39.《数据堂(北京)科技股份有限公司关于股票恢复转让的公告》,2018年9月7日。

40.《北京瑞智华胜科技股份有限公司关于公司股票在全国中小企业股份转让系统终止挂牌的公告》,2018年11月1日。

41.北京科锐国际人力资源股份有限公司。

42.广州尚品宅配家居股份有限公司。

至涉及更为严重的刑事风险,如2017年8月11日,数据堂(北京)科技股份有限公司因员工涉嫌侵犯公民个人信息罪而作出公司股票暂停转让的公告,直至2018年9月11日才恢复转让³⁹。2017年北京瑞智华胜科技股份有限公司申请新三板挂牌过程中被要求解释数据采集、使用的合法合规性问题。因涉嫌特大数据泄露案件,公司于2018年11月终止挂牌⁴⁰。2019年公司被判非法获取计算机信息系统数据罪,处罚款人民币10,000,000元。

PART II 识别风险篇

SECTION 001

企业上市的数据合规审查趋势

统计分析揭示上市企业申报过程中数据合规审核有以下的特点:

- **数据合规是全行业全领域企业所面临的普遍挑战:**不仅科技企业面临日趋严格的数据合规审查,身处传统行业的拟上市企业,如业务经营涉及大量用户数据⁴¹,或在销售设计端运用云计算与大数据技术⁴²,也会在申请上市过程中面临审核机关就数据合规相关的问题的问询。

- **审核机关的问询更加具体、有针对性。**我们注意到,在《网络安全法》颁布之初发审委的问询相对笼统和概括,关注点在于企业数据来源是否合规、是否建立内部控制制度。随着数据保护规范不断完善,发审委的问询问题逐渐具体化到企业是否建立数据供应商甄选机制,是否建立数据备份机制、防泄漏机制与到期数据处理机制等具体制度,以及该等制度是否实际得到有效执行。

- **审核机关对拟上市企业问询回复的审查更加深入。**在梳理近期拟上市企业审核问询函及回复的过程中我们发现,发审委将针对企业回复中不明晰的阐述持续追问,例如某企业在问询回复中称其产品“不曾亦不会获取用户的隐私数据”,随后发审委发起了进一步问询,要求该企业解释这一认定的依据是否充分合理。为准确回答该等问询问题,拟上市企业需对企业数据进行全面和准确的风险识别并落实相应合规措施。

- **审核机关的问询同样关注企业如何相应匹配技术性措施。**发审委针对拟上市企业系统与技术的关注体现在两个方面。一是要求企业对其信息保护技术体系进行说明,二是要求企业对其核心技术的合法合规性进

行说明,企业核心技术可能包括移动客户端技术、大规模通信技术、分布式处理技术、大数据技术以及大规模数据存贮技术等。因此,拟上市企业的数据合规治理不仅包括对数据的识别和合规风险管控,也包括对信息系统和技术的管理。

- **审核机关的问询覆盖数据全生命周期。**相较企业日常经营中采取的平衡商业需求与数据合规要求的合规标准而言,审核机关针对拟上市企业的数据合规审查标准往往更为严苛,其数据收集、使用、共享、数据安全制度、以及与商业伙伴的合作业务模式均会落入发审委审查的范围。同时,拟上市企业为满足上市披露要求,对其数据相关产品及服务模式的公开披露也将进一步扩大企业的合规风险。

SECTION 002

企业上市前应当基于具体商业模式确定数据风险

上市过程中企业的数据治理将面对发审委的全方位考察。除此之外,拟上市企业还应做好成功上市所带来的后续合规风险的规避。成功获批上市的企业将在其招股说明书中按发审委要求或自行决定披露投资者需特别关注的风险因素,该等风险披露将把企业潜在的数据风险暴露在投资者、产品与服务的使用者、以及同行业竞争者的关注之下,随之而来的可能行政处罚风险及潜在的民事侵权诉讼风险和不正当竞争诉讼风险。

因此,在上市筹备阶段,拟上市企业应当将采取有效且有针对性的数据合规治理措施纳入上市整改工作范围之内,以防范该等风险。通过对既往上市企业涉及的数据合规问询的梳理,我们整理了既往上市企业申报过程中面临的主要数据合规风险点,以期对拟上市企业开展合规治理工作有所助益。

企业一:利用大数据向移动应用开发者和广告主提供服务⁴³

风险因素: (1) 不当使用互联网信息的风险。公司通过向移动应用开发者提供第三方消息推送服务,覆盖了大量移动终端和活跃用户。虽然公司一贯重视信息数据的保护并建立了完善的信息保密制度和操作流程,但在业务开展过程中,一旦公司员工或数据合作方、客户基于自身原因造成了信息的不当使用,将会对公司声誉造成不利影响,甚至可能会对公司的业务开展造成不利影响,进而影响公司的经营业绩。(2) 数据资源安全风险。对于获取的数据,公司建设了数据管理中心机群,公司采用

44.北京值得买科技股份有限公司。

45.北京瑞智华胜科技股份有限公司、周嘉林、黄健等违法运用资金罪一审刑事判决书(2019)浙0602刑初636号。

46.上海复娱文化传播股份有限公司(831472)与北京微梦创科网络技术有限公司不正当竞争纠纷二审民事判决书(2019)京73民终2799号。

47.北京瑞智华胜科技股份有限公司。

了防火墙、数据加密等技术,以保障数据资源存储、使用的安全性、可靠性。但如果公司受到互联网上的恶意软件、病毒的影响,或者受到黑客攻击,将会影响公司信息系统正常运行,或者导致公司信息数据资源泄露、损失,从而可能会损害公司的市场声誉,对公司经营业绩造成不利影响。

企业二:运营内容类导购平台⁴⁴

风险因素:公司因用户个人信息保护不当所面临的法律及用户流失风险。作为互联网信息服务提供者,公司在经营过程中会获取用户的手机号码、家庭住址、身份证号等个人信息。根据国家相关法律法规的规定,发行人收集、使用用户个人信息应当遵循合法、正当、必要的原则,并对用户个人信息的安全负责,不得泄露、篡改、毁损、出售或者非法向他人提供用户个人信息等。若由于内部管理或外部原因造成用户信息的泄露,公司将会面临承担相应法律责任以及用户投诉和用户流失的风险。

企业三:以爬虫技术为基础非法获取数据⁴⁵

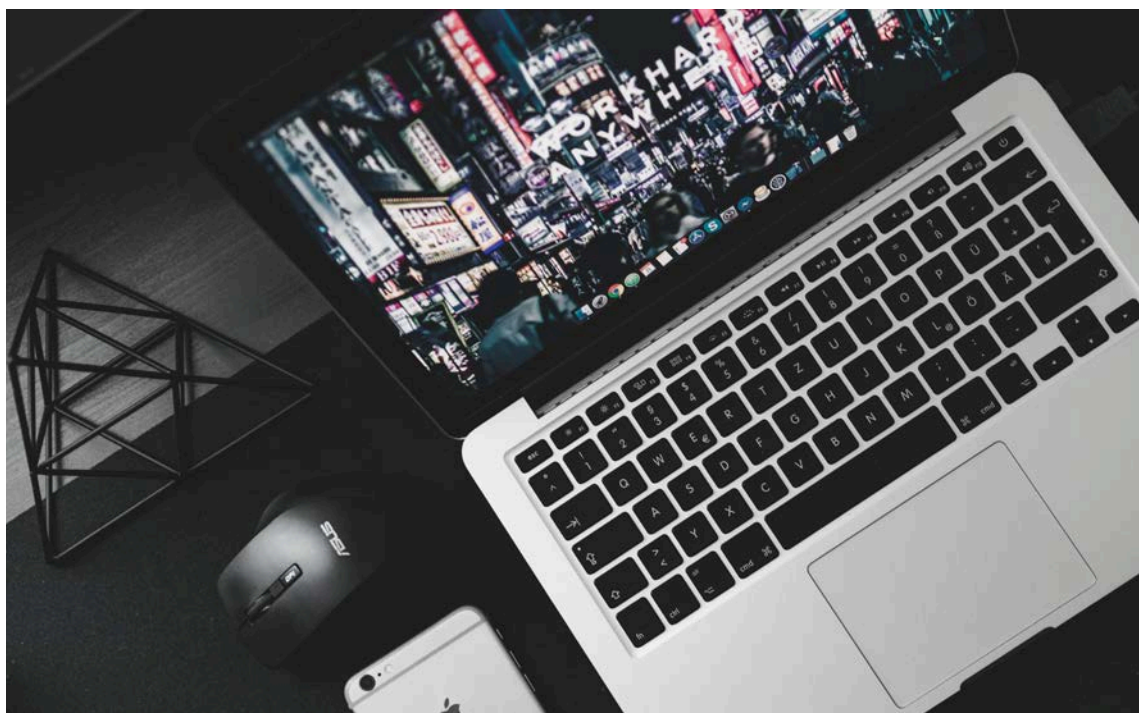
风险因素:因使用爬虫技术非法获取数据引发的刑事责任风险。公司通过股东成立的其他关联公司与运营商签订精准广告营销协议,获取运营商服务器登录许可,并通过部署SDK程序,从运营商服务器抓取采集网络用户的登录数据,并将上述数据保存在运营商数据库中,利用研发的爬虫软件、加粉软件,远程访问数据库中的数据,非法登录网络用户的淘宝、微博等账号,进行强制加粉、订单爬取等行为,从中牟利。公司该等行为构成非法获取计算机信息系统数据罪。

企业四:以爬虫技术非法爬取用户发布在第三方平台上的内容⁴⁶

风险因素:因使用爬虫技术引发的侵权与责任不正当竞争责任。公司未经许可在其运营的APP中的明星账号中设置微博专题,并嵌套该明星的新浪微博界面,完整展示该明星微博包括界面和内容在内的全部数据。

企业五:互联网新媒体营销解决方案提供商⁴⁷

风险披露:供应商相对单一的风险。公司向关联方采购占比分别达到40.16%和75.48%,对该单一供应商存在一定程度的依赖。未来如果市场发生重大不利变化或关联方因特殊原因停止向公司提供账号推广服务,可能对公司盈利能力产生较大影响。



企业六:提供大数据的存储、管理、挖掘、分析服务⁴⁸

风险披露: (1) 内部控制风险。随着公司的业务发展,公司总体经营规模将逐步扩大,这将对公司在战略规划、组织机构、内部控制、运营管理、财务管理等方面提出更高要求。股份公司设立前,公司内控体系不够健全,运作不够规范。公司整体变更为股份有限公司后,逐步建立健全了法人治理结构,制定了适应企业发展的内部控制体系。但由于股份公司运行前期缺少专业机构的辅导和督导,公司及管理层的规范运作意识不高,在实际运行中存在一定程度的不规范性。(2) 数据来源合法性的风险。公司作为一家大数据公司,业务涉及到数据的收集,如果收集到的数据涉及个人隐私、国家安全或其它非法数据,将面临法律方面的风险。

48. 数据堂(北京)科技股份有限公司。

49. 北京指南针科技发展股份有限公司。

企业七:以互联网为工具提供金融数据分析和证券投资咨询服务⁴⁹

风险披露: 互联网系统及数据安全风险。互联网及相关设备客观上存在着网络基础设施故障、软件漏洞、网络恶意攻击及自然灾害等因素引起网络瘫痪的风险。上述风险一旦发生,客户将无法及时享受公司提供的产品和服务,严重时可能造成公司业务中断,从而影响公司的声誉和经营业绩甚至引起法律诉讼。

50. 优刻得科技股份有限公司。

51. 杭州安恒信息技术股份有限公司。

52. 杭州鸿泉物联网技术股份有限公司。

企业八：第三方云计算服务商⁵⁰

风险披露：信息安全与数据保密风险。公司的各类产品服务及其赖以运行的基础网络、处理的数据和信息，可能存在软硬件缺陷、系统集成缺陷以及信息安全管理中潜在的薄弱环节，从而导致不同程度的安全风险。由于信息系统本身固有的安全特点，公司存在不可预测的信息安全与数据保密的风险，一旦发生信息安全事故，可能存在业务系统产生漏洞，客户数据泄密或流向错误，从而对公司的经营造成影响。

企业九：提供专业的网络信息安全服务⁵¹

风险因素：因最终客户发生数据泄密及其他网络安全事件时，公司承担罚款或赔偿的风险。当最终客户发生数据泄密及其他网络安全事件时，如主管部门认定公司在提供相应产品或服务时违反了国家与网络安全和信息安全相关的法律法规，公司可能承担相应的法律责任，并可能需根据销售合同的约定向客户承担相应的赔偿责任。

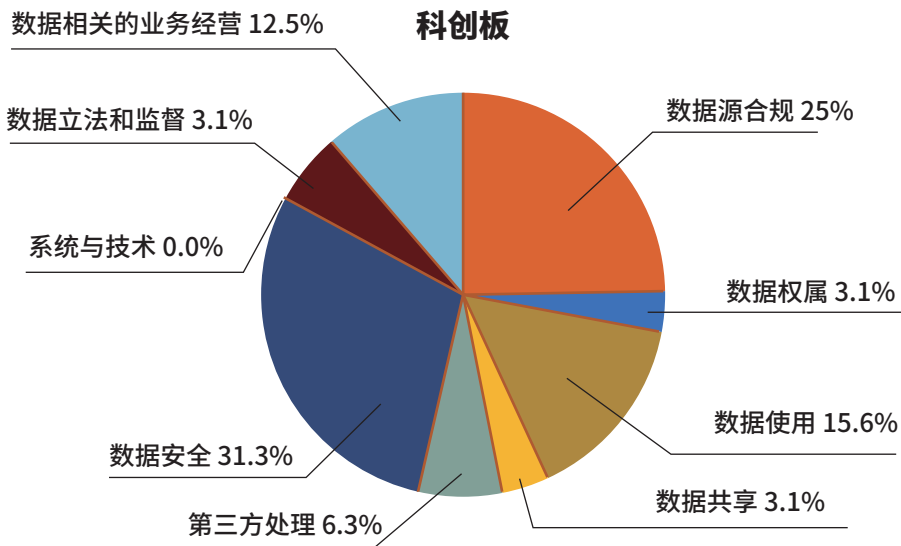
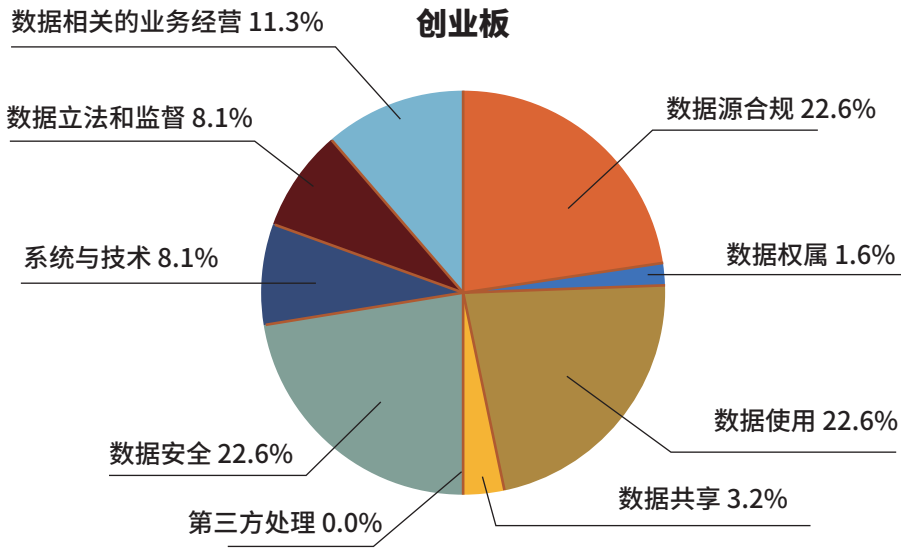
企业十：提供智慧城市业务⁵²

风险因素：公司运营业务尚未取得第三方测评机构出具的信息安全等级保护测评报告的风险。信息安全测评认证中心仍在进行测评工作，正式测评报告尚未出具，如正式测评报告的安全保护等级高于第三级以上（含第三级），则公司存在未及时进行信息安全等级保护测评而被主管部门责令改正、给予警告的风险。

PART III

数据合规治理篇

证监会发行审核委员会（“发审委”）在企业上市审核中所关注的合规问题如下图所示，结合拟上市企业将面临的数据合规审查趋势，拟上市企业如何开展数据合规治理工作，以妥善应对审核机关问询，并有效降低行政监管、民事甚至刑事风险，是我们接下来关注的重点。



表(一) 审核中所关注的数据合规问题分析

53.《网络安全法》第四十一条：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

54.《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第四条：违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

55.《网络安全法》第四十一条。

56.《网络安全法》第四十二条：网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照有关规定及时告知用户并向有关主管部门报告。

SECTION 001

明确数据合规治理目标

为有效应对上市过程中的数据合规挑战，拟上市企业应针对以下合规要求作为上市前的数据合规工作目标。

序号	类别	合规要求
1	数据源合规 (占比24%)	识别企业数据来源渠道，判断是否涉及主动收集或者用户主动提供、第三方采购、或者通过数据爬取等方式从公开渠道获取等数据来源渠道。
2		识别数据类型，判断是否包括个人信息、重要数据及其他受监管的特定行业数据。
3		根据不同数据源渠道与数据类型识别合规风险，调整相应业务模式及授权条款，以保障数据源合法性、降低合规风险。
4		直接收集个人信息的，应当在收集前明示个人信息收集使用的具体规则、获取个人信息主体的授权同意、按照法律法规及与用户之间的约定收集、存储个人信息，涉及个人信息出境的，应当落实安全评估及申报工作等 ⁵³ 。
5		从第三方采购数据的，应审核引入相应数据类型及数据量的必要性，在数据采集协议中要求数据供应商作出数据来源合法合规的承诺与保证，同时在企业内部落实《供应商数据保护合规管理制度》。坚守不得非法获取公民个人信息的刑事责任红线。 ⁵⁴
6		通过爬虫技术收集数据的，应遵守网站的Robots协议及适用的技术协议，遵守“用户授权平台+平台授权采集方+用户授权采集方”的“三重授权原则”。同时建议明确爬取前的内部审核机制及爬取后数据处理机制，避免触发侵犯公民个人信息罪、非法获取计算机信息系统数据罪等刑事责任，或侵犯第三方权益或构成不正当竞争的民事风险。
7	数据使用 (占比20%)	应当对数据采取合理的分类分级管理，并匹配相应管理制度留存数据处理记录。
8		遵循合法、正当、必要的原则，使用个人信息的目的、方式和范围不得超出个人信息主体授权同意的范围 ⁵⁵ 。
9		存在数据融合的，融合后的使用目的不应超出原有授权范围，否则应重新获得用户或数据上游合作企业的授权同意，以避免被认定为超授权范围违法使用个人信息或引发潜在违约责任。
10		使用个人信息用于个性推送或精准营销的，应获得接收方的明示同意，避免采取“一揽子授权”的概括授权获取方式。同时提供退订渠道。
11		对照《个人信息安全规范》等行业良好实践完善各产品线的个人信息使用规则，涉及使用、处理儿童个人信息的，还应当遵循《儿童个人信息网络保护规定》、《关于引导规范教育移动互联网应用有序健康发展的意见》等专门立法对应落实特定类别的数据合规策略。
12		企业内部应针对员工访问设置分级授权规则，同时应当匹配相应员工奖惩制度。

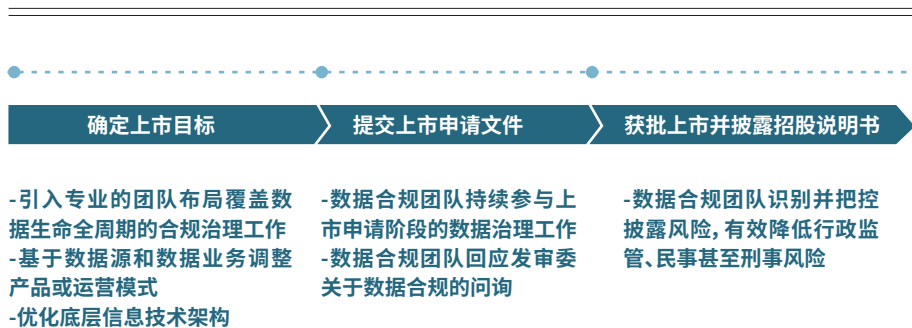
序号	类别	合规要求	
13	数据共享 (占比2.9%)	对于共享个人信息的业务而言,未经个人信息主体同意,原则上不得向他人提供用户个人信息,经处理无法识别特定个人且不能复原的除外 ⁵⁶ 。	57.《信息安全技术 个人信息安全规范》(GB/T 35273-2017) 8.2。
14		对照《个人信息安全规范》等行业良好实践,在共享个人信息前事先开展个人信息安全影响评估;向个人信息主体告知共享个人信息的目的、数据接收方的类型,并事先征得个人信息主体的授权同意;准确记录和保存个人信息共享的情况;帮助个人信息主体了解数据接收方对个人信息的保存、使用等情况,以及个人信息主体的权利 ⁵⁷ 。	58.《信息安全技术 个人信息安全规范》(GB/T 35273-2017) 8.1。
15		共享除个人信息外的其他类型数据时,应当相应识别该等共享行为所产生的风险,同时对于数据下游合作企业的数据安全能力采取一定的审核和管控措施。	59.《网络安全法》第二十一条:国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求,履行下列安全保护义务,保障网络免受干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改:(一)制定内部安全管理制度和操作规程,确定网络安全负责人,落实网络安全保护责任;(二)采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;(三)采取监测、记录网络运行状态、网络安全事件的技术措施,并按照规定留存相关的网络日志不少于六个月;(四)采取数据分类、重要数据备份和加密等措施;(五)法律、行政法规规定的其它义务。
16		对于数据融合的场景,应审核拟融合数据源的合法合规性,明确授权使用的范围,并评估融合的必要性及关联性。同时应当明确企业在数据融合过程中的控制者或处理者角色,通过明确具体合同条款、安全风险评估及定期审计等方式降低相应合规风险。	
17	第三方委托处理 (占比1.9%)	委托第三方进行个人信息处理的,应遵守《网络安全法》第四十一条规定的基本原则,确保该等第三方委托处理行为未超过个人信息主体授权同意的范围。	
18		对照《个人信息安全规范》 ⁵⁸ 开展个人信息安全影响评估,确保处理者具备足够的数据安全能力。	
19		与处理者订立数据处理协议,以厘清双方在数据保护及合规处理方面的责任义务。	
20		针对企业重点业务,应当对第三方采取一定的管控措施,落实合作前数据安全能力调研、安全风险评估,合作中定期核查,合作终妥善处理数据删除或匿名化等后续工作。	60.《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)、《信息安全技术 网络安全等级保护测评要求》(GB/T 28448-2019)、《信息安全技术 网络安全等级保护安全技术要求》(GB/T 25070-2019)。
21	数据安全 (占比24%)	按照《网络安全法》 ⁵⁹ 与“等保2.0”国家标准 ⁶⁰ 的规定开展等级保护测评工作。	61.《网络安全法》第四十二条。
22		采取技术措施和其它必要措施保护个人信息的安全,防止信息泄露、损毁或丢失。 ⁶¹	62.《网络安全法》第二十五条:网络运营者应当制定网络安全事件应急预案,及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险;在发生危害网络安全的事件时,立即启动应急预案,采取相应的补救措施,并按照有关规定向有关主管部门报告。
23		具备必要的组织机构,设立个人信息保护负责人和个人信息保护工作机构。	
24		建立个人信息收集、使用、存储、共享等全流程、全生命周期的制度,并通过培训、演练等手段予以落实。	
25		制定网络安全应急预案 ⁶² 以及及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等危害网络及数据安全的风险。	
26	系统与技 术 (占比4.8%)	采取防止外部黑客攻击的技术措施,保障企业系统安全、稳定、可靠。	
27		采取必要的加密、数据备份、数据脱敏等技术措施防止个人信息泄露与损毁。	

序号	类别	合规要求
28		可通过获得ISO 27001认证、ISO 27008认证的方式证明信息系统的安全性。
29	数据立法 和监督 (占比5.8%)	持续关注我国数据安全保护领域的立法动向和标准制定情况,值得关注的包括《个人信息保护法》、《数据安全法》等法律法规的制定,以及《个人信息告知同意指南》等国家标准的制定。
30		业务涉及数据跨境传输或跨境处理的,还应关注适用境外法律的合规情形,如欧盟《一般数据保护条例》(“GDPR”)、英国《数据保护法》、美国《在线儿童隐私保护法》(“COPPA”)、加州消费者隐私法案(“CCPA”)的合规要求。
31		持续关注国内外立法与执法动向,并合理评估及管理日益加强的数据合规监管对业务的影响。
32	数据权属 (占比2.9%)	按照《民法总则》及《民法典人格权编(草案)》对虚拟性财产权益及个人信息的人格权相关权益提出的立法原则,通过业务协议或用户协议与商业伙伴或数据主体对数据的财产性权益进行划分。
33		发现第三方不正当使用企业数据或存在其他不正当竞争行为时,依照上述协议寻求司法救济。
34	数据相关的 业务经营 (占比13.5%)	从第三方采购数据时,避免对数据供应商存在重大依赖。
35		在与业务伙伴的商业协议中加入对于潜在安全泄露的责任约定与免责条款。
36		商业协议中避免出现可能造成侵权的业务条款。
37		根据不同业务场景和数据类型设计相适配的数据保护条款或协议,以代替传统的保密条款或保密协议。

表(二)数据合规治理工作目标

SECTION 002

布局数据生命全周期的合规治理工作



表(三)拟上市企业数据合规治理流程图

上市申报及上市披露过程无疑将拟上市企业置于“聚光灯与放大镜”之下,相应的数据合规工作将是周期长、标准严苛的整体治理需求。拟上市企业在递交上市申请前往往会开展一系列的重组计划,决定上市主体、制定资产剥离方案时拟上市主体的合规程度是必须考虑的因素之一。而以数据作为核心资产的科技企业往往具有营业收入高、成本支出低的特点。高营收普遍依赖于数据源与关联公司得以实现。

这种情况下,拟上市企业为达到上市合规要求,需要基于数据源和数据业务调整产品或运营模式、优化底层信息技术架构、完善数据生命全周期合规制度,这些工作并不是一蹴而就的。而这些合规工作的完成度影响着上市主体的选定与资产剥离方案的推进。因此,从确定上市这一长期目标之始,拟上市企业应当着手布局覆盖数据生命全周期的合规治理工作。

SECTION 003

上市全流程持续引入数据合规专业团队

发审委对企业数据合规制度的问询呈现出技术性强、覆盖面广的特点,问询具体到拟上市企业的某一特定组织制度或技术措施,及数据收集、使用、存储、共享、委托处理、数据安全等数据生命全周期活动。如拟上市企业应对发审委的问询回复与实际运营情况存在出入还将受到发审委的进一步追问。

在上市过程中数据合规审查日趋严格的环境下,拟上市企业应当部署专业的数据合规团队持续参与上市全流程,在上市前期继续落实数据治理工作,在上市过程中应对发审委审核问询,在上市披露阶段把控披露风险。一方面,专业的数据合规团队能够有效将上市前针对各数据相关产品及服务的数据全流程的合规调研、数据源合规性审查、合规差距分析、合规风险识别、内部合规制度建设、对外数据合作协议完善等工作成果贯穿到上市筹备过程中,夯实数据收集、使用的合法合规性基础,为上市申请文件对核心产品与服务的释明提供依据。另一方面可以专业、客观的分析意见回应发审委的问询,凸显拟上市企业数据相关产品和服务的核心技术及商业价值,助力企业成功上市。同时,上市披露过程中专业数据合规团队可以有效识别并把控披露风险,减小企业上市后的风险敞口。

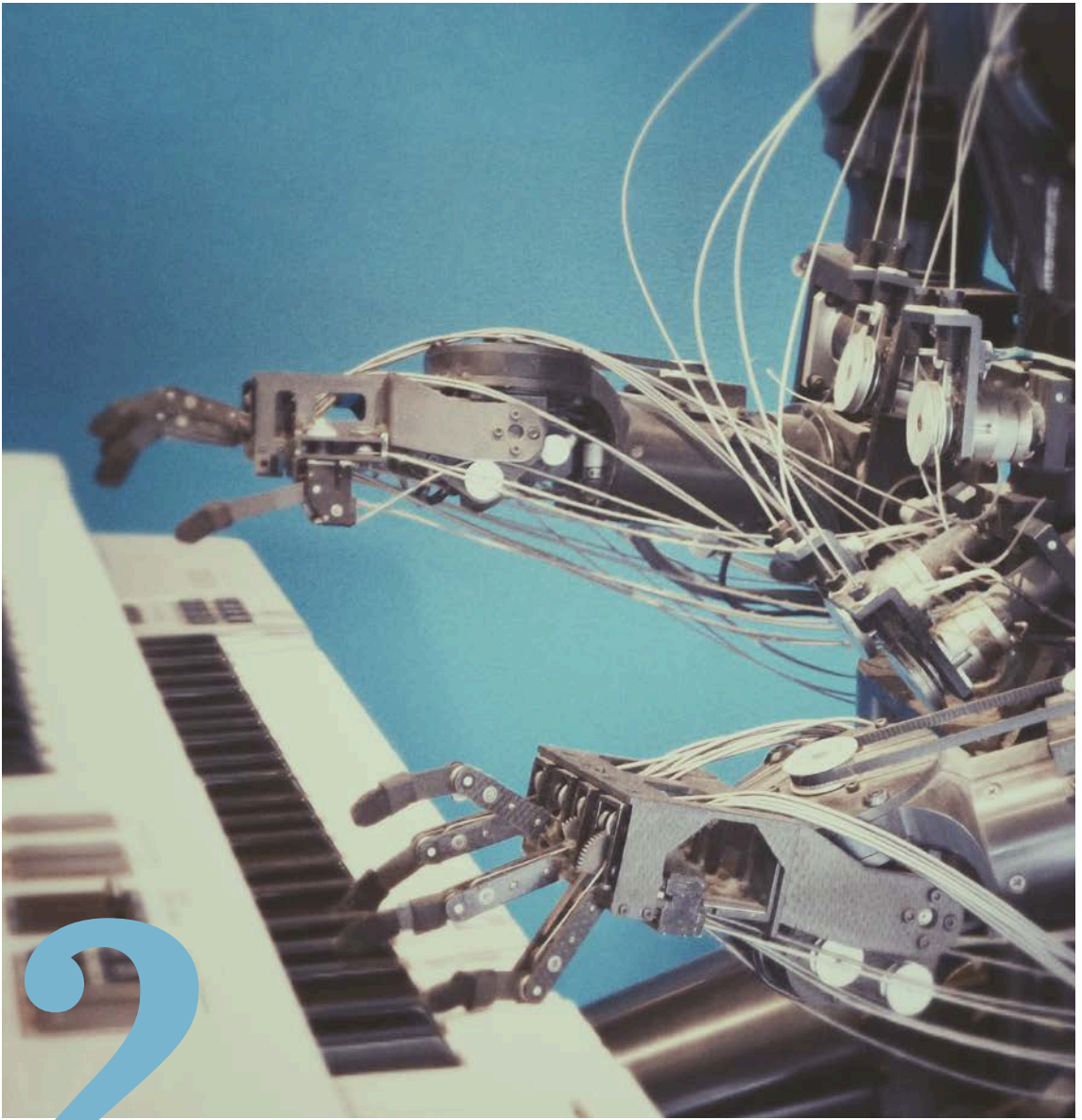
SECTION 004

结语

通过对既往上市企业申报及重组过程中涉及的数据合规相关问询的梳理,可以发现审核机关针对拟上市企业数据合规审查呈现更为全面、深入、频繁、严格的整体趋势。全行业全领域企业,尤其是科技企业,应提前布局数据合规治理工作以应对企业上市过程中面临的数据合规审查挑战。我们将结合在网络安全与数据保护领域的广泛实践经验,持续推出系列文章,对立法及政策走向及时进行解读,降低企业上市的数据合规风险。



陈际红/合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com



2

CHAPTER 04

人工智能之间达成“垄断协议”？ 算法合谋的反垄断法律风险分析

作者:薛熠/杨壹凯/俞炜

人工智能经历近年来的巨大发展,已经开始引起交通、物流、教育、医疗等各行各业的深刻变革,更是在近期“升级”为一种新型基础设施,赋能我国经济发展,进一步融入人类日常生活,以无与伦比的高效完成各种各样不可思议的任务,成为人们学习、工作中不可或缺的得力助手。但正如Melvin Kranzberg教授所提出的六大科技定律之首——“技术并无好坏,但亦非中立”,人工智能同时也带来法律和社会伦理方面的问题,引发各界人士的热烈探讨。其中,人工智能达成“垄断协议”已非妄语,而是切实地成为了人们关注的重点法律问题之一。

SECTION 001

人工智能与算法合谋

1. 人工智能与算法的关系

人工智能是什么?不同时代、不同行业的人可能对此存在不同角度的理解。在人工智能的经典教科书《人工智能:一种现代的方法》中,作者Stuart Russell与Peter Norvig认为,人工智能是有关“智能体(Intelligent agent)研究与设计”的学问,而“智能体是指一个可以观察周遭环境并做出行动以达目标的系统”。

观察当前人工智能的发展热潮,机器学习、深度学习是两个绕不开的热点词汇。人工智能、机器学习、深度学习之间又是什么关系?从非专业人士角度简单说明¹:

◆机器学习是实现人工智能的一种方法,是指基于能够自主、反复从数据中学习的算法设计智能体;

◆深度学习是当前众多机器学习方法中的热门方法之一,是基于模拟人脑神经网络进行学习、分析的算法设计智能体。

近年来人工智能的崛起,离不开机器学习,特别是其中深度学习的迅速发展。基于深度学习的应用,各种机器辅助功能都已经或即将被逐步实现。深度学习,作为有史以来最为有效的机器学习方法,是目前人工智能研究的主流技术。不同于传统机器学习的线性结构的算法,深度学习神经网络层次结构的算法下,凭借大量的训练数据和强大的计算能力所构建的深度学习模型具有更加强大的学习能力,能够更好、更快地解决更多的问题。

然而,有趣的是,深度学习的运用更像是一个不求甚解的实用主义者的做派。很多情况下,人们通常只能观察运算结果,了解深度学习模型是否能够有效工作,但即便是其设计者本人也难以明确地解释该种算法运行的具体过程。深度学习算法因此也被形象地喻为只可意会不可言传的“黑箱”。这也引起了部分人对于“人工智能失控”的担心,如果仅能知道计算机的学习成果而无法明确掌握其学习过程,那这种学习本身会不会失控?计算机会不会悄悄通过算法学到什么我们不希望它学会的知识?

2. 人工智能达成“垄断协议”?

人工智能达成“垄断协议”听起来像是未来科幻世界中的场景,但其与现实之间的距离可能并不如一般人想象的那么遥远。随着价格算法在

1. 参见OECD资深竞争法专家Antonio Capobianco在国际竞争网络(International Competition Network)于2019年1月16日召开的一次网络研讨会上所作演示, <https://ec.europa.eu/competition/cartels/icn/capobianco.pdf>.

2.例如2017年9月13日,OECD开展“算法与合谋”主题的圆桌论坛;2017年11月16日,澳大利亚竞争和消费者委员会(ACCC)主管Rod Sim就“合谋的机器人”主题做了发言;2018年10月8日,英国竞争和市场管理局(CMA)就“价格算法促进合谋和定制化定价”主题发布了研究报告;2018年10月31日,美国联邦贸易委员会就“算法、人工智能、预测性分析”主题开展研讨会等。

3.参见Algorithmic Collusion in Cournot Duopoly Market: Evidence from Experimental Economics, <http://export.arxiv.org/pdf/1802.08061>。

4.参见Artificial intelligence, algorithmic pricing and collusion, https://www.tilburguniversity.edu/sites/tiu/-files/download/Pastorello%20-%20Qlearning_3.pdf。

现代商业中的大量运用,人工智能达成“垄断协议”,也即价格算法合谋,是作为算法所引发的重要的反垄断法问题之一,已经引起各国反垄断执法机构和相关组织的关注²。

从当前的研究成果来看,价格算法合谋可以大致分为三类:

(1)明示价格算法合谋:经营者通过明示的协商沟通,就价格算法达成合谋以期实现价格垄断,价格算法是实现与维持合谋之工具;

(2)默示价格算法合谋:经营者之间不存在明示的意思联络,而通过认可相互之间的依赖性以实现和维持合谋,价格算法则是经营者认可相互依赖性的关键工具;

(3)虚拟合谋:即便经营者并无合谋意图,其采用的价格算法会在无需人为干预的状态下进行高效的反复试验,最终达成经营者之间的合作性均衡,实现合谋的效果而损害消费者利益。

在一项明示价格算法合谋和默示价格算法合谋中,价格算法作为经营者实现、维持合谋或认可相互依赖性的工具,合谋的意志仍然出自经营者自身,因而称其为“经营者利用人工智能达成‘垄断协议’”更为贴切。而在一项虚拟合谋中,价格算法自发地达成合谋的结果而不论使用该等算法的经营者是否有合谋的意图,因而,可谓是名副其实的“人工智能达成‘垄断协议’”。

SECTION 002

虚拟合谋的反垄断法风险

1. 虚拟合谋或已/或将成为现实威胁

尽管当前算法如何具体实现合谋效果,以及当前实践中是否已经发生了此类合谋尚不明确,但各国反垄断执法机构和相关组织对虚拟合谋的担心并非空穴来风,这从各地学者所进行的一些极具启发性的研究中便可见一斑:

(1)价格算法或能迫使市场经营者与其合谋

在2018年浙大的一份论文³中,作者设计了一种可以导致合谋的算法,并在理论说明之外采用了实验经济学方法,进行该算法与真人博弈的实验,最终得出结论——该等算法确实可以迫使真人与其进行合谋,实现超竞争水平的价格行为。

(2)价格算法之间或能自主达成合谋

在2018年博洛尼亚大学学者所著的一份论文⁴中,作者在计算机模拟

环境下,设置2到4个经营者使用相同价格算法进行了价格行为实验,发现即便是极为简单的价格算法也能够学习、实施复杂的合谋策略,对竞争对手以及自身的定价行为作出反应,并最终达成合谋的结果。

(3) 市场经营者难以达成默示合谋

与前述涉及价格算法的经济学实验不同,以真人作为对象的定价行为实验相关文献⁵表明,如果没有明示的交流,真人之间很难协调达成合谋。真人之间的默示合谋大多只能发生于极为简单的市场条件下,例如,双寡头垄断市场。此外,即便是在类似的理想化的简单市场结构下,真人达成合谋的情况也存在不确定性。

“积极向上”的人工智能的远大前程无人能及⁶,而“误入歧途”的人工智能从事合谋的手段也可能远比最狡猾的商界巨鳄来得更加精明。价格算法合谋问题,尤其是虚拟合谋,最引人担忧之处正在于此——能够在不需要人为干预的情况下,通过自主学习达成合谋,而这一过程可能鲜有痕迹可寻。更明确地说,即便没有价格算法设计者的专门设计和价格算法使用者的明确指令,价格算法也能够完全陌生的市场环境中,不通过市场信息的沟通而仅依靠自主学习的过程掌握、实施复杂的合谋策略。

5.例如Two are few and four are many: number effects in experimental oligopolies. How Much Collusion? A Meta-Analysis On Oligopoly Experiments等文献, <https://www.sciencedirect.com/science/article/abs/pii/S0167268103001380>, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=951160。

6.例如,基于深度学习的AlphaGo棋力早在几年前就已经被公认超过人类职业围棋顶尖水平而成为棋王。

7.例如,医疗行业中运用算法所导致的医疗事故、交通运输行业中运用算法所导致的交通事故等。

2. 虚拟合谋的反垄断规制亟待更多研究

是否需要以及如何从反垄断法角度对虚拟合谋进行评价与规制的疑问目前尚无定论,仍有待更多的理论与实践观察。

就技术角度而言,“黑箱”中的价格算法如何在学习过程中掌握、实施合谋策略,以及目前市场上是否已经存在此类算法合谋还有待观察。此外,如前所述,虚拟合谋的达成过程可能鲜有痕迹可寻,而仅能从效果上进行观察,如何对虚拟合谋进行有效观测也是一大技术难题。

就法律规范角度而言,首先需要解决的便是虚拟合谋的归责原则问题。由于虚拟合谋的达成并不以经营者的合谋意图及意思联络为前提,虚拟合谋所涉经营者在无主观过错的情况下是否需要承担责任?该等责任又如何能在价格算法的设计者和使用者之间进行公平、合理的分配?事实上,这也不仅仅是价格算法合谋需要解决的问题,也是任何其他“算法事故”共同面临的难题。

由于缺乏相应的技术工具,通过价格算法实现经营者之间“心照不宣”的过程更是难以发现、监测、证明、认定。

SECTION 003

经营者利用人工智能达成算法合谋的反垄断法风险

相较于前述虚拟合谋的远景,“经营者利用人工智能达成‘垄断协议’”的反垄断法风险,即上文所述的明示价格算法合谋和默示价格算法合谋,对于各国执法机构和经营者来说是眼下更为迫切的关注点。

1. 明示价格算法合谋

明示价格算法合谋的问题相对简单,可以适用一般经验法则——若不涉及算法的某一行为本身违法,那么即便涉及算法的元素也不会改变该等行为的违法性。事实上,对于明示价格算法合谋而言,算法仅仅是作为实现、维持合谋之工具,并未触及、改变明示合谋的实质,因而并不会落于传统反垄断法规制框架之外,由各司法区域通过价格卡特尔予以规制。

2. 默示价格算法合谋

默示价格算法合谋的问题则相对复杂一些。在包括美国、欧盟等在内的大多数司法区域内,传统的默示合谋均尚未被视为违法而受到规制,原因主要有二:其一,基于“心照不宣”而实现的默示合谋不仅由于缺乏明示的协商沟通而难以达成,且由于缺乏相应约束机制而容易瓦解;其二,基于“心照不宣”而实现的默示合谋即便在实践中发生,也难以发现、证明、认定。

就该等原因的本质而言,价格算法本身对默示算法合谋的反垄断法风险产生了重大影响,使得其更易实现、维持且难以被发现、证明、认定:

◆价格算法一定程度上导致市场结构性变化,为经营达成对相互依赖性的认可提供隐秘的手段,更有利于合谋的产生,且算法的应用可以作为及时、有效监督价格背离行为的手段,更有利于合谋的维持;

◆由于缺乏相应的技术工具,通过价格算法实现经营者之间“心照不宣”的过程更是难以发现、监测、证明、认定。

因此,对默示价格算法合谋的反垄断法规制,目前仍缺少相应的制度工具以及有效的技术工具。尽管如此,考虑到默示价格算法合谋的反竞争效果与明示合谋相比并无不同,且默示价格算法合谋相比于传统默示合谋更易发生且难以观察,各反垄断司法区域对默示合谋监管的节制、容忍态度或将发生改变。

SECTION 004

企业应该怎么做才能避免人工智能之间达成“垄断协议”的风险？

价格算法合谋对市场竞争的威胁并非虚无缥缈，在更多理论研究与实践观察的基础上，如何从立法、执法和司法反面跟进、解决这一竞争威胁是各个反垄断司法区域共同关心的话题。价格算法合谋的反垄断法规制正是山雨欲来，企业也应当未雨绸缪，在使用价格算法作为商业工具、享受技术红利的同时，也应当对价格算法的潜在反垄断法风险有所注意：

- ◆企业应当避免出于合谋的目的，设计或者使用价格算法，企业记录设计、使用价格算法商业决定的独立性以及合理性将大有裨益；
- ◆企业自行设计并使用价格算法应当注意保密，警惕价格算法构成竞争性敏感信息的可能，更不应在竞争者之间传递、交换和交流；
- ◆企业使用第三方设计的价格算法应当全面关注市场上其他竞争者使用相同算法的情形，避免无故受到牵连；
- ◆企业应当将价格算法的应用纳入企业反垄断合规管理体系之内，价格算法还可能导致合谋之外的反垄断法风险（例如，价格歧视等），企业全面、谨慎的合规意识十分必要；以及，
- ◆企业关注技术进步改善商业决策的同时，也应当关注各司法区域反垄断立法、执法和司法的最新发展动向，以便掌握先机，防患未然。



薛熠 / 合伙人
公司二部
北京办公室
+86 10 5957 2057
xueyi@zhonglun.com



CHAPTER 04

**“大数据从何而来”，
涉足大数据业务需留意的
“网络爬虫”技术的合规风险**

作者:薛熠/杨壹凯/程若锦

在“新基建”的风口下,大数据分析和应用不可或缺:无论对于物联网、人工智能,还是智能交通,亦或是商业领域的分析点击流量、客户质量、智能定价等等,莫不如此。随着《网络安全法》及其配套法规、标准及规范性文件的陆续发布,大数据业务更加成为学界、法律工作者、媒体及大众关注的重点,尤其在2019年,不断传出某些大数据业务经营者,因“过度收集、非法窃取和贩卖个人数据信息”、“未经个人同意搜集个人数据信息”等被警方调查或被迫下架的消息。同时,大数据公司也在担忧:大数据分析的业务该如何开展?如何合法合规地收集数据?哪些技术可以使用?

本文将搜集大数据的技术之一,网络爬虫技术为例,讨论网络爬虫技术在使用和应用中的重点法律合规问题,供从事大数据业务的企业参考。

SECTION 001

网络爬虫织网,为大数据分析捕捉信息

1、什么是网络爬虫

网络爬虫/爬虫程序(Web Crawler),也称网络机器人(Web robots)、网络游客、蜘蛛爬虫,根据《互联网搜索引擎服务自律公约》,这是一种按照指定规则,可自动、批量从互联网爬行抓取数据信息的程序。网络爬虫技术作为采集大数据的主要方式之一,和重要的大数据信息来源,已经被广泛并成熟地应用于各种互联网商业模式和使用场景,例如:新零售、社交、新闻、地图、互联网金融等。

基于不同的使用场景,网络爬虫可以分为通用爬虫和专用爬虫:

◆通用爬虫主要应用于搜索引擎服务,其主要工作是无特定目标随机地抓取海量网页内容并下载到本地,储存为镜像快照并识别网页文字关键词;

◆专用爬虫为爬取特定范围的网页而设计,使用者可以设置一个爬取的主题或范围,通过图像识别、机器学习等技术的帮助,爬取互联网上的特定内容。

2、网络爬虫与大数据的联系

网络爬虫爬取的数据是大数据企业数据分析的重要源头之一,例如:一些大数据分析企业开发的“购物平台大数据分析软件”会借助爬虫技术大量收集购物平台的信息,如买家关键词搜索热度、某关键词引向的成交量、某关键词产品的定价分布等等,当收集到足够多的原始信息样本后,再借助大数据分析技术,向其客户提供商品流行趋势、定价策略的分析;一些信用调查公司也是运用网络爬虫技术,从渺如烟海的互联网信息中识别并抓取特定主体的信用相关信息,进而通过对大数据的分析,相应得出信用结论。

SECTION 002

网络爬虫合规风险分析

通过网络爬虫技术爬取到的数据信息有以下几种分类方式:(1)按照数据可得性,可以分为公开网络数据信息和非公开网络数据信息(如需付费观看的信息,或是内部数据库信息);(2)按照数据归属主体,可以分

1. 通常而言,“反爬虫安排”包括以下三类:
 (1) 在IT支持团队中设置专门的反爬虫团队并开发阻止爬虫脚本自动运行的“墙”,比如设置需要滑动进行验证或需要按次序点击的验证码等;在内容格式加密上做文章,比如采取将关键数据转为图片,或采用JavaScript混淆技术等。
 (2) 爬虫的“潜规则”,例如,爬虫使用方主动约束爬虫的爬取吞吐量,避免因爬虫造成的访问量过载导致网站瘫痪。
 (3) 在网站中挂出机器人协议文件(robots.txt),该协议是网站的所有者通过明示的方式,对不同主体派出的爬虫进行授权,写明可访问和不可访问的文件信息而制定的爬虫行为准则。机器人协议并非也不能直接用技术手段阻止爬虫进行数据搜集,缺乏强制性,但业内普遍认为,制定机器人协议应当是行业内的通行规则,没有遵守协议的行为明显不当,应当在发生争议时承担相应的不利后果。



为个人信息数据、企业商业数据和社会公开数据。

目前,我国还没有已经生效的针对应用网络爬虫技术的规范性文件,从事大数据业务的企业在评估和分析其网络爬虫技术手段是否合规,可以从以下几个方向考虑:

- (1) 爬取数据的行为是否合规;
- (2) 爬取的数据本身是否存在合规问题;以及,
- (3) 爬取数据之后对数据的使用及存储等是否合规。

1、爬取数据的行为是否合规

网络爬虫技术采取的是“广撒网”模式,爬虫脚本自动运行后,在确定的爬取网站范围内对各网站上载的信息进行遍历。但基于商业利益等因素的考量,部分网站的部分/全部数据信息是不允许其他主体爬取的,因而会选择通过制定和公布机器人协议(robots协议)或通过设置技术性障碍或通过平台服务协议等方式来限制或禁止外部爬虫访问特定的数据信息。该等措施通常被称为“反爬虫安排”¹。尽管存在反爬虫安排,但有些企业还是会绕过或无视这些反爬虫的规制,进而给其自身带来合规风险,主要包括被认定为未经授权(包括网站授权和个人授权)收集数据、导致网站无法正常运营,构成犯罪的,还可能需要承担刑事责任(如非法侵入计算机信息系统罪、破坏计算机信息系统罪、非法获取计算机信息系统数据罪等)。

为方便阅读,我们将上述爬取数据的行为可能导致的企业合规风险以下表展示:

序号	合规风险	法律责任	
1	未经网站授权收集数据：若被爬取数据的网站并未开放或授权数据采集，以爬虫方式收集数据信息的行为可能会违反机器人协议或侵犯网站其他相关权益	民事责任： (1) 侵犯著作权或其他民事责任 (2) 构成不正当竞争	司法实践中，法院认为，机器人协议应当被认定为搜索引擎行业内公认的、应当被遵守的商业道德，是数据权利人针对爬虫方的一种维权途径，以明示禁止爬取行为；如果爬虫方不遵守机器人协议，未经网站授权，其收集数据行为明显不当，可能构成侵权或不正当竞争 ² 。在无前述机器人协议的情况下，网站作为权利人，可以主张爬虫方侵犯著作权 ³ 或构成不正当竞争 ⁴ 。
		刑事责任	严重的未经网站授权爬取数据行为可能会构成犯罪，比如侵犯著作权罪 ⁵ 、非法获取计算机信息系统数据罪 ⁶ 、非法侵入计算机信息系统罪。
2	未经个人授权收集数据：在爬虫方通过网络爬虫技术收集个人信息时，可能被界定为《网络安全法》项下的网络运营者，进而需根据《网络安全法》和《信息技术个人信息安全规范》（GB/T 35273-2017） ⁷ 等规定，在收集个人信息前，获得个人信息主体的授权同意；间接获取个人信息时，应向个人信息提供方了解个人信息主体是否授权同意转让、共享、公开披露等	民事责任	爬虫方未经个人授权收集自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等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自然人个人身份的各种信息，或超范围过度收集个人信息的，可能因违反《网络安全法》、《信息技术个人信息安全规范》和/或《互联网个人信息安全保护指南》，而被要求承担侵权责任。
		行政处罚	爬虫方未经个人授权收集个人信息的，或超范围过度收集个人信息的，可能违反《网络安全法》第四十一条，企业和直接负责的主管人员和其他直接责任人员分别被处以责令改正、警告、没收违法所得、罚款，甚至责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。 若爬虫方取得的信息为非公开渠道的信息，涉及窃取或者以其他非法方式获取个人信息，将可能面临被没收违法所得，并处罚款。
		刑事责任	爬虫方未经个人授权收集能够识别公民个人身份或者涉及公民个人隐私的个人信息的，可能被认定为是“窃取或者以其他方法非法获取公民个人信息”，构成侵犯公民个人信息罪 ⁸ 。
3	导致网站无法正常运营 ⁹ ：因爬虫导致网站负荷过大，大量正常用户请求堵塞，访问出现速度慢或部分页面无法显示等现象。	民事责任	如果使用爬虫技术导致网站无法被正常访问，可能构成侵权并承担对网站经营者所遭受损失的侵权赔偿责任。
		刑事责任	如果使用爬虫技术获取信息被认定为对计算机信息系统功能进行干扰，造成其不能正常运行，则可能触犯破坏计算机信息系统罪。

2. 见“浙江泛亚电子商务有限公司诉百度在线网络技术(北京)有限公司等侵犯著作权纠纷案”一审民事判决书，案号：(2006)一中民初字第6273号；“百度与奇虎公司不正当竞争纠纷案”一审民事判决书，案号：(2013)一中民初字第2668号。

3. 见“亚长城影视文化(北京)有限公司与精伦电子股份有限公司侵犯影视作品著作权案”，案号：(2014)鄂民三终字第00107号。

4. 见“深圳市谷米科技有限公司与被告武汉元光科技有限公司、邵凌霄、陈鼎、刘江红、刘坤朋、张翔不正当竞争”民事判决书，案号：(2017)粤03民初822号。

5. 见“何超侵犯著作权案”，案号：(2016)沪03刑终1号。

6. 见“邵凌霄、陈鼎、刘江红、刘坤朋、张翔犯非法获取计算机信息系统数据罪案”，案号：(2017)粤0305刑初153号。

7. 国家标准化管理委员会及国家市场监督管理总局已于2020年3月6日发布新版《信息安全技术 个人信息安全规范》(GB/T 35273-2020)，但新版规范于2020年10月1日正式实施，目前仍需参考《信息技术个人信息安全规范》(GB/T 35273-2017)。

8. 见“秦帅等侵犯公民个人信息罪案”，案号：(2018)京0108刑初770号。

9. 我国目前正在研究出台《数据安全管理办法》，在已公布的征求意见稿中提出，网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

若爬取的数据中包含个人信息，
爬虫方对该等个人信息的使用
应当取得明确授权同意使用的
范围和使用目的。

2、爬取数据的合规性

爬虫方除应当评估其数据爬取行为是否合规外，还应当评估和分析其爬取所得的数据本身是否可能侵犯他人的权利，例如：涉及个人信息保护、侵犯著作权或商业秘密。

10.见“北京微梦创科网络技术有限公司与北京淘友天下技术有限公司等不正当竞争案”一审民事判决书，案号：(2015)海民初字第12602号。

11.参见 <http://finance.caixin.com/2019-10-22/101474132.html>，“北京金融局摸排区内大数据公司爬虫业务”。

<p>侵犯个人信息与隐私权</p>	<ul style="list-style-type: none"> ◆爬虫方在某网站(以下称“信息提供方”)爬取到他人的个人信息时,可能需要进一步确认信息提供方是否取得相应的授权,转让、共享、公开披露该等个人信息。若否,信息提供方可能涉及超授权范围使用个人信息,而间接获取个人信息的爬虫方也因存在过失而涉及未经授权收集个人信息。 ◆所爬取的个人信息涉及隐私的,还可能侵犯其隐私权。
<p>侵犯著作权/构成侵犯著作权罪</p>	<ul style="list-style-type: none"> ◆爬虫方在进行抓取网页信息时,若将他人作品复制保存,可能会侵犯他人的复制权。 ◆若爬虫方在保存爬取到的数据时,抹去了他人署名或进行删改,可能侵犯他人的署名权、修改权。 ◆在爬虫方以营利为目的,未经著作权人许可,复制发行其文字作品、音乐、电影、电视、录像作品、计算机软件及其他作品的,根据违法所得数额和是否具有严重情节的,还可能被认定为侵犯著作权罪。
<p>侵犯商业秘密</p>	<p>若爬虫方获取的数据信息符合我国《反不正当竞争法》项下对商业秘密的定义,即不为公众知悉、具有商业价值并经权利人采取相应保密措施的商业信息,且这类爬虫行为可能被认定为是电子侵入或以其他不正当手段获取,则可能会被认定为侵犯他人的商业秘密。¹⁰</p>

3、爬取数据之后对数据的使用及存储等是否合规

在爬虫方已合规取得数据信息的情况下,企业还应当留意其后续使用、存储该等数据信息是否合规,例如:是否存在超范围使用、侵犯著作权、不正当竞争、信息泄露等问题。

<p>超范围使用爬虫数据</p>	<ul style="list-style-type: none"> ◆有些网站可能会在网页中添加法律声明、权利归属或版权保护条款,对数据的权利归属和使用限制进行声明,爬虫方应当在后续使用所爬取的数据时,在前述类似声明的允许框架内合理使用数据。 ◆若爬取的数据中包含个人信息,爬虫方对该等个人信息的使用应当取得明确授权同意使用的范围和使用目的。 ◆对爬取的数据的使用应当恰当,避免出现以下情况:因某些大数据信用调查公司利用爬虫技术搜集个人信息并用于暴力催收,而导致该等企业被警方调查或应金融主管部门的要求进行自查整改。¹¹
------------------	---

12. 见“上海汉清信息咨询有限公司与爱帮聚信(北京)科技有限公司、爱帮聚信(北京)信息技术有限公司不正当竞争纠纷一案”民事判决书,案号:(2010)海民初字第24463号。

13. 在实践中,有一种情形较为多见:视频网站爬取其他网站的视频信息,在自己的网站上提供播放服务,或小说网站“盗取”正版小说网站的收费作品,在自己的网站上免费供网友阅读,这些情形均可能涉及侵犯著作权人的信息网络传播权。

不正当竞争	企业在使用通过爬虫技术取得的同类网站相关信息且直接不加修改地使用数据时,可能被认定为搭便车、构成混淆等不正当竞争行为。在司法实践中,法院认为,通过爬虫技术手段获取其他同类网站付出人力、物力、财力和时间等运营成本搜集整理的信息数据后,直接在自己的网站上展示并以此获取商业利益的行为,因未付出劳动、未支出成本、未做出贡献,属于反不正当竞争法理论中典型的“不劳而获”和“搭便车”的行为;同时,由于使用内容完全一致,使用爬虫数据的一方可能会对同类网站构成实质性替代,这种经营模式违反公平原则和诚实信用原则,违反公认的商业道德,构成不正当竞争。 ¹²
侵犯著作权	爬虫方在使用所收集的涉及他人著作权的数据内容时,应注意不得实施抹去权利人的信息、对作品进行不当剪裁等行为 ¹³ ,否则可能侵犯权利人的复制权、署名权、修改权、信息网络传播权等著作权。
未能保证爬虫数据信息安全	企业在保存获取的数据信息时,爬虫方应当严格遵循《网络安全法》对网络安全等级保护制度的要求、防止网络数据泄露或被窃取、篡改,也应当符合存储大数据的互联网数据中心的建设标准,采取技术措施和其他必要措施,保证其收集及保管的数据信息的安全。

SECTION 003

企业合规建议

1、作为爬虫方

- (1) 注意其他网站的机器人协议的具体内容和限制;
- (2) 严格管控数据采集的范围,不超范围采集,当涉及个人信息的需格外慎重;
- (3) 使用过程中需要甄别爬虫收集的信息的权属,确保对信息权利人著作权、个人信息等的保护,并确保不超范围使用;
- (4) 不得将爬虫技术及采集到的数据信息用于不正当竞争或其他缺乏合理性、合法性的用途;
- (5) 当抓取的信息侵犯其他方权益时,应及时通知相关方删除、断开或自行删除、断开使用该等侵权数据的链接;
- (6) 在存储爬虫所收集的数据时,应当注意信息安全。



薛熠 / 合伙人
公司二部
北京办公室
+86 10 5957 2057
xueyi@zhonglun.com

2、作为反爬虫方

- (1) 组建专业的信息安全团队;
- (2) 编制合理的机器人协议,将其内容合同化,同时注意不得利用机器人协议进行不正当竞争行为;
- (3) 合理利用爬虫技术监控互联网中的其他主体是否有不合理使用自己的数据信息的情况。



4

CHAPTER 04

外商投资“新基建” 需要注意哪些监管问题

作者:蒋蕙匡

2020年起施行的《外商投资法》及相关配套制度改革旨在完善外商投资营商环境,便利外商投资流程。适逢新冠疫情导致全球经济整体下行,“新基建”领域或将成为外国投资者在华投资的新机遇。据估计,本轮“新基建”投资规模可达上万亿,其中外商投资占比将达到8%左右¹。

当然,考虑到“新基建”项目本身的特点,外国投资者在某些领域的具体投资交易中可能需要受制于特殊的监管要求,本文将简要梳理外商投资“新基建”领域中应当注意的监管问题,主要包括外商投资准入特别管理措施、国家安全审查和反垄断审查三个方面。

1. 参见国金证券研究所:“新基建”的体量到底有多大”,访问地址:<http://finance.sina.com.cn/stock/hyyj/2020-03-12/doc-iimxy-qvz9791194.shtml>。

SECTION 001

外商投资准入特别管理措施(《外资负面清单》)

根据国家发改委明确的“新基建”范围，“新基建”领域将涵盖制造业、交通、能源、信息技术等多个行业，并呈现出多行业相互融合的特点，如“融合基础设施”即强调传统基础设施在与互联网、人工智能等信息技术行业融合的基础上实现转型升级。而根据《外商投资准入特别管理措施(负面清单)》(2019年版)(“《外资负面清单》”)，“新基建”领域涵盖的部分行业，例如“信息传输、信息传输、软件和信息技术服务业”等(“**限制类行业**”)，将很可能落入外商投资准入特别管理措施范围内。

具体来说，在三类新型基础设施中，信息基础设施和融合基础设施都将依托于信息技术，故投资这两类基础设施需要关注是否属于涉及限制外资进入的电信行业。例如：5G、卫星互联网等通信网络基础设施的运营通常要依托大规模公共网络基础设施，属于须由中方控股的基础电信业务；数据中心、智能计算中心等算力基础设施的运营通常构成互联网数据中心(IDC)和数据处理(EDI)等业务形态，属于外商投资股比不得超过50%的增值电信业务²，而智能交通基础设施、智慧能源基础设施等融合基础设施的运营通常涉及数据处理和信息平台的搭建，构成在线数据处理(EDI)和信息服务(ICP)等业务形态，亦属于外商投资股比不得超过50%的增值电信业务。

因此，对于外国投资者而言，一方面，其在非限制类行业的现有投资项目在向上述两类新型基础设施转型升级的过程中，有可能会落入限制类行业范围而受制于外资准入特别管理措施。此时，外国投资者将可能面临无法作为控股或全资股东的问题，或者在已经全资或控股持有投资项目权益的情况下，需要退出项目或减少权益以满足监管要求，或者就受限的部分与中国合作伙伴设立新的商业存在。另一方面，其未来投资上述两类新型基础设施(包括将其在境外的此类平台在华落地)时，也必须采用适当的交易方案，以满足相应外商投资特别管理措施要求，例如与本土的合作伙伴成立合资企业、搭建VIE架构、剥离轻重资产等。

而创新基础设施，相对于上述信息基础设施和融合基础设施，更侧重于“重”资产层面，例如大型科研装置、实验室等重大科技基础设施、孵化器、科技产业园等产业技术创新基础设施，主要涉及技术服务、商业服务和房地产等行业。根据《外资负面清单》，除少数科学研究和技术服务领域外³，除非与上述受制于外资准入特别管理措施的业务形态进行融

2. 对于互联网数据中心(IDC)业务而言，根据现行外资准入政策，目前仅允许符合《〈内地与香港关于建立更紧密经贸关系的安排〉服务贸易协议》和《〈内地与澳门关于建立更紧密经贸关系的安排〉服务贸易协议》(CEPA)条件的港澳投资者在中国大陆设立合资企业取得IDC牌照，且在合资企业中的持股比例不应超过50%。我们注意到，实践中，已有多个中外合资的数据中心项目已在CEPA项下取得增值电信业务经营许可证，涉及NTT、SAP等国际知名的电信行业运营商。

3. 具体包括人体干细胞、基因诊断与治疗技术开发和应用以及地理测绘、调查和地图编制等领域。

4. 比如已经在中国活跃多年的外国投资者如高通、SAP、英特尔、霍尼韦尔等均表示新基建将给在华外企带来更多的机遇,并且纷纷加码投资布局相关领域,参见“新基建”带来新机遇——外企加码谋求合作共赢”。
访问地址:
http://www.dzww.com/xinwen/guoneixinwen/202005/t20200502_5673460.htm。

合,创新基础设施行业的投资本身涉及外资准入特别管理措施的可能性较小。

相比之下,在范围更广的泛“新基建”领域,外国投资者面临的准入要求要更少。例如,新型基础设施的上游产业链(如通信产品、芯片、智能装备、技术解决方案等)和下游产业链(如智能产品等),在《外资负面清单》中已经基本不存在外商投资准入特别管理措施,而目前也已经有诸多外国投资者在这些领域活跃多年并且正在加码布局新基建相关领域⁴。

SECTION 002

外商投资(国家)安全审查

“新基建”系指新型的基础设施建设,而基础设施建设很容易联系到国家经济安全的行业(甚至国防事业),因此,除《外资负面清单》项下一般性外商投资准入特别管理措施外,“新基建”领域的外商投资也需要基于个案评估是否受制于(国家)安全审查。

外商投资(国家)安全审查始于国务院办公厅于2011年2月3日发布《关于建立外国投资者并购境内企业安全审查制度的通知》(“《国务院安全审查通知》”)。今年施行的《外商投资法》中再次明确了对影响或者可能影响国家安全的外商投资进行(国家)安全审查的要求。

根据《国务院安全审查通知》,受制于安全审查的外商投资分为两类,具体如下表所示:

类别	涉及国防安全	非涉及国防安全
具体类型	<ul style="list-style-type: none"> •产品:军工及军工配套企业 •地点:位于重点、敏感军事设施周边 •关系国防安全的其他单位 	<ul style="list-style-type: none"> •重要农产品 •重要能源和资源 •重要基础设施 •重要运输服务 •关键技术 •重大装备制造 •关系国家安全的其他行业 •重要文化、重要信息技术产品和服务(仅适用于自贸区)
触发条件	并购	并购+获得实际控制权

对于第一类涉及国防安全的,只要外国投资者直接或间接获得该等企业的资产或股权,即触发安全审查要求;对于第二类非涉及国防安全的,需要外国投资者通过并购获得该企业实际控制权,才触发安全审查要

求。尽管如此，监管部门在认定特定投资是否属于安全审查范围上拥有广泛的自由裁量权。

对于三类新型基础设施，根据上述宽泛的规定，不排除由于落入“重要基础设施”“关键技术”“重要信息技术产品和服务”等领域而纳入考察范围，实践中需要根据个案投资活动情况判断是否涉及国家安全，并视情况与监管部门进行沟通。

此外，从外商投资交易类型上来说，近年来的立法趋势正在将受制于国家安全审查的“并购”的概念拓展为范围更广的“外商投资”。就自贸区而言，2015年《关于印发自由贸易试验区外商投资国家安全审查试行办法的通知》不仅规定受制于国家安全审查的交易类型由“并购”拓展为“投资”，同时也正面地将“协议控制、代持、信托、再投资、境外交易、租赁、认购可转换债券等方式投资”纳入审查范围。更重要的是，目前已经实施的《外商投资法》也明确了要进行安全审查的范围是“外商投资”。因此，未来的安全审查体系很可能将适用于所有外商投资交易类型，而不仅限于一般的并购类交易。

就安全审查程序而言，外商投资安全审查工作由外国投资者并购境内企业安全审查部际联席会议（“联席会议”）具体负责，联席会议属于非常设机构，由国务院领导，国家发改委与商务部牵头，根据外资并购所涉及的行业和领域还可能由不同的其他部门共同组成。自2019年5月起，国家发改委具体负责安全审查相关的商谈、受理申请、提交审查、反馈审查决定等工作⁵。关于安全审查的周期，根据相关规定，在正式受理后的审查期限通常不超过90个工作日，但是对于受理前审查却没有特定的时限要求，因此安全审查的整个流程在实践中可能长达数月。

因此，对于外国投资者投资新基建领域而言，有必要将外商投资（国家）安全审查的评估和申报纳入整体的交易计划之中，以免投资交易在实施阶段因安全审查的监管要求而受到阻碍⁶。

5. 根据公开信息，2019年8月21日，永辉超市（601933, SH）宣布其于当日收到国家发改委通知要求其就要约收购中百集团（000759, SZ）的交易进行外商投资安全审查。随后，于2019年12月16日，永辉超市宣布取消了部分要约收购中百集团的计划，维持29.86%的持股比例不变，不再谋求中百集团的实际控制权。据悉，这是国家发改委在接替商务部主管外商投资安全审查窗口职能后获得首次公开报道的涉及国家安全审查的并购案件。

6. 我们对外商投资安全审查制度和趋势的解读，参见“外商投资安全审查2.0时代即将到来？”一文，访问地址：<http://www.zhonglun.com/Content/2019/09-04/1647363311.html>。



SECTION 003

反垄断审查

根据《反垄断法》，当投资交易构成经营者集中并达到申报标准时，投资交易将会受制于事前的反垄断审查（“反垄断审查”）。相较于前述两项监管要求，反垄断审查并非专门针对外国投资者，对于不具有排除、限制竞争效果的交易而言也不会造成实质性的阻碍。事实上，绝大多数提交反垄断申报的交易都能够获得无条件的批准。因此，对于外国投资者而言，在交易早期进行反垄断申报的评估，并依法依规进行申报，将能够保证投资交易顺利推进。

具体针对新基建领域的外商投资活动而言，其反垄断审查也可能涉及如下较为特别之处：

从交易的相关市场界定和竞争分析来看，由于新型基础设施大多依托互联网技术，具有多边平台的属性（即面向多类需求群体），在涉及此类新型基础设施的案件中，由于业态新颖，或者与传统业态之间的竞争关系难以准确界定，或者相关领域的竞争者数据难以获得，可能导致相关市场界定以及相关经营者的市场支配力的评估存在难度，从而给审查

周期和结果带来变数,但是另一方面,交易方也可以因此基于自己的行业经验提出更为灵活的主张和判断,引导监管思路随着行业本身的更新换代而“与时俱进”。

从交易架构上来说,在某些限制外商投资的领域,实践中存在不少公司采用VIE结构规避外资准入的风险。由于涉及VIE的交易往往处于监管的灰色地带,国内反垄断执法机关对此的态度较为保守或不甚明朗,相关交易能否获得批准甚至能否立案具有较大的不确定性。然而,随着国内市场经济的发展和监管环境的变化,我们注意到执法机关对于这一问题的处理方式似乎也开始变得灵活,例如对于交易方原架构涉及VIE而交易本身不涉及外资准入限制的案件,执法机关似乎并未拒绝按正常程序立案审查⁷。这在一定程度上反映了执法机关近年来对于VIE结构态度的变化,涉及VIE结构的交易仍有获得正常立案、批准的可能性,且未来执法机关对于相关交易未依法申报的调查处理也可能趋严。该等执法动态对于外国投资者采用VIE架构投资“新基建”领域的反垄断申报会产生何种影响,还有待进一步观察。

此外,根据近年来的案例,反垄断审查、国家安全审查以及证券监管机关对涉及上市公司交易的审查程序等往往是可以并行的,而并非互为条件。值得注意的是,实践中,反垄断审查往往是监管部门深入了解交易背景以及与其他政府审批进行“联动”的绝好机会。例如,反垄断审查的执法机构(过去为商务部,机构改革之后为国家市场监管总局)是安全审查联席会议的组成部门,并且国家市场监管总局在反垄断审查过程中,可根据需要主动征求有关政府部分以及其他单位或个人的意见。此外,反垄断审查申报表中也要求申报人披露该交易是否需要中国政府其他部门审批。

随着国家大力推动“新基建”相关产业的发展,“新基建”领域可能成为外商投资的又一个“风口”。在国家进一步扩大对外开放,积极促进外商投资,推动形成全面开放新格局的大背景下,外商投资“新基建”领域也将适用更加公正、透明、健全的监管体系。除了外商投资准入监管以及相应的在投资架构方面的考虑,外商投资者也需要根据具体投资方向重点关注新基建领域投资并购项目后续的日常运营相关的合规要求,比如商业模式的合规、相关业务经营许可证的获得、数据保护和网络安全合规、数据以及其他互联网产品和服务定价政策合规等诸多方面。我们建议外国投资者们能够深入了解相关的监管要求,积极跟进新的监管规定,以便高效、合规地在“新基建”领域开展外商投资活动。

7. 参见上海明察哲刚管理咨询有限公司与环胜信息技术(上海)有限公司新设合营企业案之简易案件公示表,访问地址:
http://www.samr.gov.cn/fld-j/ajgs/jzjya-jgs/202004/t20200420_314431.html。



蒋蕙园/合伙人
公司部
北京办公室
+86 10 5957 2131
jianghuiyuan
@zhonglun.com



5

CHAPTER 04

智能家居出海的 八个数据保护关键词

作者:陈际红/吴佳蔚/杨润

随着“互联网+”的深入发展,传统家居行业不断探索新的发展路径,在更新硬件技术的同时拓展“软件定义并融入硬件”的智能家居路线¹。目前国内众多智能家居厂商纷纷瞄准海外市场。鉴于智能家居设备在为用户提供服务时需要通过智能摄像头、智能音箱等收集、处理大量数据,智能家居的隐私安全问题逐渐引起公众重视。此外,全球范围内数据保护立法及执法日趋严格,对个人数据保护提出了更为具体的、严苛的要求。因此,国内智能家居厂商在开拓海外市场时,应当充分重视个人数据保护,使个人数据保护合规成为产品出海的标准配置。

本文以目前域外监管框架相对完善、违规后果最为严重的欧盟《一般数据保护条例》(GDPR)合规要求为基础,结合监管重点、用户关注热点及行业实践,提炼出八个智能家居出海的数据保护关键词:知情、合法、必要、联动、安全、跨境、交互、趋势。

1.前瞻产业研究院,《预见2019:2019年中国智能家居产业全景图谱》,

资源来源:<https://www.qianzhan.com/analyst/detail/220/190702-41750a1f.html>,最近访问时间:2020年4月4日。

SECTION 001

关键词一/知情:如何确保用户充分知情,满足透明性的要求?

根据GDPR项下的透明性原则,在处理个人数据前应当以简明易懂的方式告知个人数据主体其个人数据处理的相关信息,确保个人数据主体知情。

与一般网页端、APP端产品可直接向用户展示隐私政策不同,智能家居设备在向用户告知时存在以下典型难点:①从内容上来看,智能家居产品涉及的技术功能较为复杂,所收集的个人数据种类繁多,导致用户理解起来相对困难³;②从形式上来看,部分智能家居设备没有屏幕且不具备语音交互等功能,只能通过纸质说明书等方式对用户进行告知⁴。部分设备为向用户提供完整高效的服务,可能会被集成到其他设备当中,无法实现单独告知。此外,整体来说,目前国内大部分智能家居隐私政策透明度较低,普遍缺失某些重要条款⁵,若不及时整改,出海时必将面临较大的合规风险。

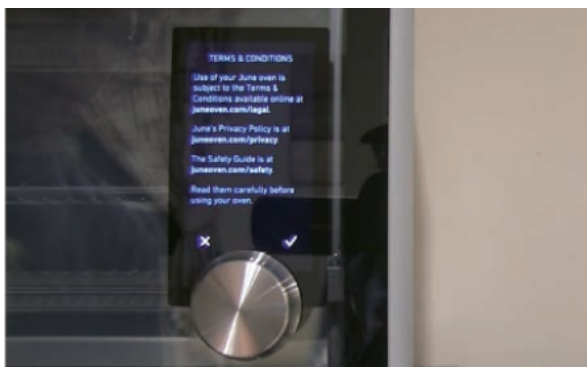
考虑到上述难点,为保障用户知情权的实现,充分满足透明性的要求,企业可参考以下途径完善产品隐私政策:①内容上:全面完整地梳理产品功能,充分说明各功能所对应收集处理的个人数据、收集目的、是否涉及共享、可能存在的风险等;适当地对技术术语等较难理解的词汇进行阐释,方便用户理解。②形式上:可与APP连接、有展示屏幕或具备语音交互等功能的智能家居产品,可以以屏幕显示、语音提示等方式呈现;不具备上述特点的,一方面可在产品官网上以显著方式提示用户阅读隐私政策,或在产品介绍、说明文件中附上隐私政策,另一方面在产品上可以添加链接至隐私政策的二维码,并提示用户阅读隐私政策。

2. Joseph Lindley, Paul Coulton, Haider Ali Akml, Brandin Hanson Knowles, "Anticipating GDPR in Smart Homes Through Fictional Conversational Objects", Computer Science, 2017, P13.

3. European Commission, "IoT Privacy, Data Protection, Information Security (working document)", 资料来源: https://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753, 最近访问时间:2020年4月4日。

4. 中国信息通信研究院,《“互联网+行业”个人信息保护研究报告》,2020,第23页。

5. 南都个人信息保护研究中心,《2018年互联网个人信息保护合规观察报告》,资料来源: <http://www.oeeee.com/nis/201810/12/570175.html>, 最近访问时间:2020年4月4日。



某品牌智烤箱隐私条款展示界面²

6.Hihome, Hihome Privacy Policy, 资料来源: <https://www.hihome.eu/en/service/privacy-policy/>, 最近访问时间: 2020年4月5日。

SECTION 002

关键词二/合法:如何保证数据处理活动具备合法依据?是否必须征得用户同意?



某智能家居产品隐私政策中对法律基础的说明⁶

根据GDPR项下的合法性原则,所有数据处理活动均需具备适当的法律基础。根据GDPR第6条,法律基础主要包括数据主体同意、履行所必要、履行法律义务所必要、保护自然人利益、维护社会公共利益及正当利益。

对于智能家居产品所进行的数据处理活动而言,与其他产品或服务一致,均需根据数据处理活动的具体情况判断所依据的法律基础。通常来说,企业进行数据处理活动所依据的法律基础主要为用户同意、履行所必要及正当利益。

针对适用用户同意为法律基础的数据处理活动(例如可对睡眠状况、心率等健康状况进行监控的智能床、使用指纹或人脸进行解锁的智能门锁以及精准营销等),需注意GDPR项下的同意应为用户主动作出的、针对具体行为的、建立在用户充分知情基础上的、可随时以简便的方式撤回的明确意思表示,企业应当以满足上述要求的方式征得用户同意;针对适用履行所必要为法律基础的数据处理活动(例如能够自动控制温度的热水器等一般类型的家电产品),企业应当注意完善产品使用条款或其他面向用户的合同文本,涵盖实现产品基本功能所需收集的数据的相关描述,确保该等收集没有超出基于合同提供服务最小必要的范围,不超出用户的合理期待;针对适用正当利益为法律基础的数据处理活动,企业需及时进行利益平衡测试,确保已采取了适当的组织和技术措施,保证实现企业的商业利益不会减损用户的基本权利和自由。

SECTION 003

关键词三/必要:如何实现在最小必要的范围内处理个人数据?

根据GDPR项下的目的限制原则及数据最小化原则,个人数据的收集

和处理应当具有具体、明确的目的,且应仅限于实现目的所需的最小限度内进行处理。

相较于一般的互联网产品,智能家居产品所进行的数据处理活动为实现上述目的所面临的挑战主要包括:物联网(Internet of Things, IoT)本身需要多个数据库之间的匹配与比对,智能互联就代表着无限潜在活动的可能链接,因此需要判断所发展出的新功能是一项全新的功能还是已有功能的合理扩展⁷。以智能运动手表为例,用户同意设备基于监测其健康状况的目的收集其心率、运动轨迹等数据,但企业若将该等数据进行自动化决策分析进而向其发送定向广告则明显超出了用户同意所涵盖的处理范围。

为判断可能存在的风险,保证智能家居产品所进行的数据处理活动充分符合目的限制原则及数据最小化原则的要求,企业应当进行风险评估,基于评估结果确定数据最小化的实现方式,并应嵌入在系统开发的全生命周期中⁸。

SECTION 004

关键词四/联动:如何对合作第三方的个人数据处理活动进行管理?

根据智能家居行业研究报告显示,随着智能家居平台之间整合力度的不断加强,有近一半的设备能够同时接入两个或以上的智能互联平台。同时,语音助手服务资源也将不断整合,更多的家居设备将搭载语音助手⁹。

7. Bridget Treacy, Anita Bapat, "The 'Internet of Things' —already in a home near you?", 资料来源: <https://www.hunton-ak.com/images/-content/3/4/v3/3421/The-Internet-of-Things-already-in-a-home-near-you.pdf>, 最近访问时间:2020年4月5日。

8. Nominet, "Privacy guidelines for IoT — what you need to know", 资料来源: <https://www.nominet.uk/privacy-guidelines-for-iot-what-you-need-to-know-infographic/>, 最近访问时间:2020年4月5日。

9. IDC, 《中国智能家居市场2020年十大预测——市场将进入规模化发展阶段》, 资料来源: <https://www.idc.com/getdoc.jsp?containerId=prCHC45788719>, 最近访问时间:2020年4月5日。

10. "Developer Preview of Local Home SDK", 资料来源: <https://developers.google.com/assistant>, 最近访问时间:2020年4月5日。

Figure 1 shows a successful fulfillment and execution of a smart home EXECUTE intent.



通过Google home控制其他第三方设备方式的简要说明¹⁰

11. David Priest, "Smart home developers raise concerns about Alexa and Google Assistant security", 资料来源: <https://www.cnet.com/news/smart-home-developers-raise-concerns-about-alexa-and-google-assistant-security/>, 最近访问时间: 2020年4月5日。

12. Rambus, "Smart Home: Threats and Countermeasures", 资料来源: <https://www.rambus.com/iot/smart-home/>, 最近访问时间: 2020年4月5日。

13. Matthew James, "Smart Home Cyber Security", 资料来源: <https://www.cyberdefensemaga-zine.com/smart-home-cyber-security/>, 最近访问时间: 2020年4月5日。

部分智能家居企业在开拓海外市场时,会选择在Google home、Amazon Alexa等受众较广的智能家居平台上进行开发,以云对云的技术控制方案来实现对设备的语音控制。在此过程中即涉及到三方主体(用户、智能家居厂商及智能家居语音平台)之间的数据交互,部分仅提供硬件及后台运维开发的厂商甚至会涉及到四方或以上主体之间的数据交互,因此,要充分明确各方之间,尤其是厂商及平台之间关于数据处理活动的权责义务。

在实践中,企业一方面要选择个人数据保护合规能力及安全技术水平较高的平台进行开发,严格遵循各项开发协议及要求,推动相关主体之间数据处理协议的签署。另一方面则是要不断提高研发能力和设备的安全水平,避免出现合作平台暗中截留数据进行其他目的处理的情况。¹¹。

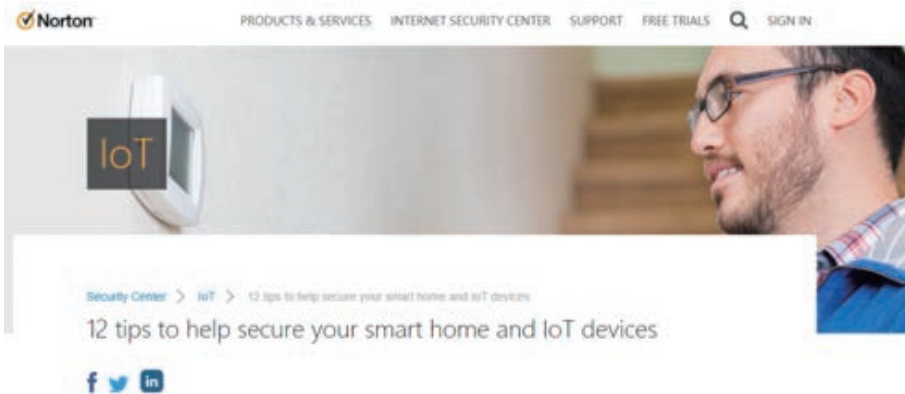
SECTION 005

关键词五/安全: 如何保障个人数据安全?

由于智能家居是以住宅为平台,利用综合布线技术、网络通信技术、安全防范技术、自动控制技术及音视频技术将家居生活有关的设施集成,构建高效的住宅设施与家庭日程事务的管理系统,各项设备或平台之间通过蓝牙、网关等进行互联,存在较大的信息安全风险。

智能家居产品所面临的信息安全风险主要来源于三方面:首先,来源于外部攻击,例如攻击者破坏、数据和身份窃取、设备劫持等¹²;其次,来源于设备或平台本身,例如设备本身在上线前未进行充分的安全性测试,存在明显的安全漏洞或者后台数据库未进行安全加固,导致数据泄露等;最后,来源于用户自身,部分用户对于复杂的安全技术缺乏充分的认识,导致未意识到可能存在的安全隐患¹³。

由于国内部分智能家居厂前身为传统家电制造商,在信息安全方面的经验和能力相对较为薄弱。基于上述风险及企业面临的实际情况,企业可从以下几个要点入手,不断提高安全风险控制水平:在高层重视、资源投入及人员投入等方面加强信息安全能力建设及安全事件应急处理能力提升,并在相对成熟时申请ISO 27001等信息安全认证;从产品设计及开发阶段即融入安全考虑,对产品进行充分的安全检测;通过产品说明、官网公告、所互联的APP等方式向用户提示安全风险,告知其基本的安全措施等。



14. “12 tips to help secure your smart home and IoT devices”, 资料来源: <https://us.norton.com/internetsecurity-iot-smart-home-security-core.html>, 最近访问时间: 2020年4月5日。

某智能家居品牌在官网上提示用户保障设备安全的方法¹⁴

SECTION 006

关键词六/跨境:如何合规地将个人数据传输至中国境内?

根据GDPR第五章,个人数据跨境传输既包括物理上跨越国境发生转移的情形(指个人数据在地理位置上、空间上发生的物理转移,既包括通过网络发生的转移,也包括通过物理载体将个人数据从一个国家/地区带到另一国家/地区的转移),还包括个人数据被远程访问的情形。在进行个人数据跨境传输时,首先需明确传输双方的基本信息及所在法域,其次是要明确进行数据传输的目的和合法依据,确保具备适当的传输安全保障机制。

基于上述规定,国内智能家居企业在面向海外用户提供产品及服务时,无论是将数据直接回传在至境内,还是在当地架设服务器或租用云服务器后境内人员进行远程访问,基本都会涉及个人数据的跨境传输。

针对不同的数据跨境方式,企业应当视实际情况采取不同的合规措施:对于从产品终端或当地服务器直接将个人数据回传至境内的情形,一方面要在隐私政策中充分告知其相关信息并在必要时征得个人数据主体的同意,另一方面可以结合业务的实际需要适度控制回传数据的规模和频率,同时可以采取技术措施对数据进行加密或脱敏、匿名化处理等;对于远程访问的情形,除在隐私政策中进行说明、必要时征得个人数据主体同意等以外,涉及租用第三方服务器的,还应当与该等第三方签署数据传输协议,同时限制访问人员范围及权限等,避免发生数据安全事件。

15. Article 29 Data Protection Working Party, “Opinion 8/2014 on the on Recent Developments on the Internet of Things”, 资料来源: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, 最近访问时间: 2020年4月5日。

SECTION 007

关键词七 / 交互: 如何保障用户行使个人数据相关权利?

根据GDPR, 数据主体享有知情权、访问权、更正权、删除权、可携带权、反对权及限制处理权, 数据控制者或处理者应该具备相应的机制支持数据主体行使其权利, 并在规定时间内对其权利请求进行响应。

由于智能家居产品本身的特点, 在支持个人数据主体行使权利时面临着以下困难: 首先, 如“关键词一 知情”所述, 部分智能家居设备没有屏幕且不具备语音交互等功能, 用户没有易于操作的方式行使其权利; 此外, 由于智能家居产品可能涉及到对非用户的个人数据的收集和处理, 此类主体行权尚存在一定困难¹⁵。

为充分保证数据主体权利的实现, 对于有屏幕或互联APP的产品, 企业应当设置相应的功能供用户行使其权利; 对于其他类产品, 应当在隐私政策中进行充分的说明, 提供邮箱、电话、邮寄等方式以使用户行权。在企业内部, 应当建立起完整的数据主体权利请求响应机制或流程并提高相应的技术能力, 对用户的权利请求进行及时、高效的响应。

SECTION 008

关键词八 / 趋势: 智能家居个人数据保护合规的发展趋势是什么?

根据GDPR第25条, 设计的隐私保护(Privacy by Design)是指在决定数据处理的目的及方式时, 即应考虑采取适当的组织和技术措施, 并在处理中整合必要的安全保障措施, 以实现了对数据处理基本原则的遵守以及对数据主体基本权利和自由的保障; 默认的隐私保护(Privacy by Default)则是应当采取适当的组织和技术措施以保障在默认情况下只有为特定目的所必要的个人数据被处理, 二者统称为设计和默认的隐私保护(Privacy by Design and Default, PbD)。根据GDPR的要求, 在数据处理活动全流程中均应贯穿PbD的各项要求, 全面履行数据保护基本原则, 在产品开发初始阶段即应充分考虑各项合规要求。

主动而非被动反应, 预防而非补救 Proactive not Reactive; Preventative not Remedial.	设计的隐私保护是主动的而非被动的事先反应措施, 用以预防和防止隐私侵入事件, 而非事后补救措施。
默认隐私 Privacy as the Default Setting	确保在任何给定的IT系统或业务实践中自动保护个人数据。
隐私嵌入设计 Privacy Embedded into Design	隐私设计嵌入到IT系统和业务实践的设计和架构中。
正而非零和 Full Functionality: Positive-Sum, not Zero-Sum	隐私设计旨在满足所有的合法利益和目的, 而不是通过零和的方法, 进行利益权衡, 舍弃某些功能。
端到端的安全, 数据全生命周期保护 End-to-End Security: Full Lifecycle Protection	在数据收集前, 隐私设计应嵌入到系统中, 并扩展到所涉及的个人数据的整个生命周期中, 保障隐私安全。
可视性和透明性 Visibility and Transparency: Keep it Open	隐私设计保证所有相关者的操作行为都可以被独立地验证, 并且对于用户和产品提供者都是可见且透明的。
尊重用户隐私, 以用户为中心 Respect for User Privacy: Keep it User-Centric	隐私设计的目的是为了保护个人的基本权利和自由, 所采取的措施应当以尊重其隐私为核心。

PbD 核心理念¹⁶

新技术的应用引发了智能家居产品一系列个人数据保护问题, 却也是解决这些问题的关键¹⁷。越来越多的智能家居厂商开始考虑并着手将产品设计之初便融入PbD的要求, 以减少产品的隐私漏洞及后续添加升级时的高昂成本。企业在考虑将PbD要求融入产品设计及数据处理的全生命周期时, 可以参考以下良好实践: 在全流程中, 重点关注数据假名化及数据最小化的技术实现, 同时采取其他组织和技术措施, 例如加密传输、加密存储、权限控制、培训提升员工意识及技术能力等。

16. Ann Cavoukian, Ph.D, "Privacy by Design: The 7 Foundational Principles", Information & Privacy Commissioner Ontario, Canada, 资料来源: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>, 最近访问时间: 2020年4月5日

17. Martin J Kraemer, William Seymour, Reuben Binns, Max Van Kleek, Ivan Flechais, "Informing The Future of Data Protection in Smart Homes", 资料来源: <http://www.cs.ox.ac.uk/files/11111/workshop-iotdirections.pdf>, 最近访问时间: 2020年4月5日。

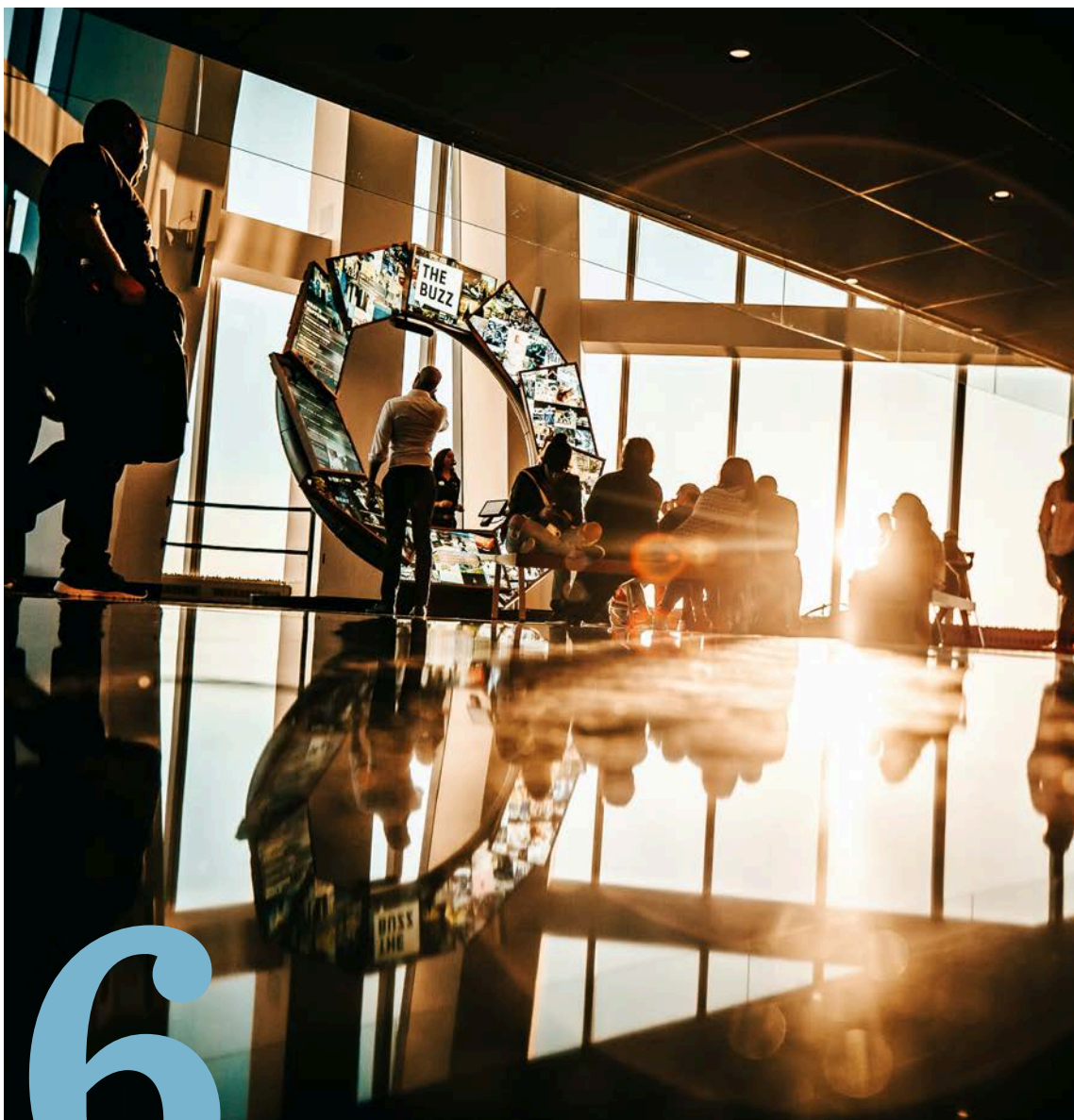
SECTION 009

结语

5G和人工智能技术发展助推智能家居产品的更新迭代,中国智能家居企业在不断开拓海外市场的同时也应当充分关注个人数据保护合规问题,在参考本文八个关键词的基础上,结合自身海外市场规划,逐步建立内部个人数据保护体系,打造外部的隐私保护形象,使个人数据保护合规能力成为开拓海外市场的关键竞争优势和重要助推力量。



陈际红/合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com



6

CHAPTER 04

移动互联网产品跨境出海 的合规风险与对策

作者:蔡鹏/闫莹/薛泽涵

随着人工智能、大数据技术及云计算能力的推广运用,在日渐纯熟的移动通信技术的推动下,互联网技术正在加速各地区各领域信息和数据的互联互通。越来越多的国内互联网企业在巩固境内竞争优势的同时,着眼于海外市场的扩展建设,发力于移动互联产品的出海落地。此外,国内市场日趋饱和以及新冠疫情的出现,一定程度上助推国内企业加快移动互联产品的海外布局和推广落地。

移动互联网服务和产品具有传播速度快、传播范围广等特点,产品和服务一旦上传至网络,短短几小时内就能传播至世界各地,其推广效率远远超过了传统工业产品。而移动互联网的这些新优势,往往也会使企业面临更多的不可控因素和法律风险。

根据我们的服务经验以及团队的服务特点,我们特选取了与移动互联网产品密切相关的落地资质、数据合规及知识产权问题作为本篇主要讨论的内容。

SECTION 001

落地资质

“落地资质”板块,包括电信运营资质及产品认证,系决定移动互联网产品是否能在特定国家或地区落地并正常运营的直接因素。互联网企业在推进产品海外布局时,应着重评估此板块要求,调研了解本企业产品进入当地市场的难度及限制,探寻合法有效的应对措施。

1. 运营资质

(1) 所需牌照识别

鉴于移动互联产品通常需依赖本地或远程互联网(局域网)或通讯网(或两者同时运用)以保持正常运营,可能涉及运营或者使用本地电信资源,而电信资源通常由所在国家或地区进行管控及有序分配,因此不同国家或地区,对于境外移动互联产品的进入,可能会采取不同程度的准入限制。确定产品落入本地电信服务监管范围,并认准产品本地运营所需的电信相关牌照,对于出海企业而言属于首要核心工作。

判断是否需要获取特定电信牌照,以及需要怎样的电信牌照,需严格按照本地电信监管要求,并结合产品自身在应用环境、产品功能、技术特征等方面的情况,进行匹配评估。通常而言,评估逻辑包括如下:

方面	要素	结论
应用环境	1. 产品所投入运用的环境,是否包括或者限定于勘探、军工、海运等特殊行业领域。	如是,产品可能同时或仅受制于本地电信管理法规以外的、特殊行业的法规要求。对此,需先评估产品是否落入本地电信监管范围,并同时了解特定行业对类似产品是否有其他准入门槛要求。
	2. 产品是否向本地企业及个人等不特定用户提供服务,或者仅限于特定范围用户进行内部使用。	如仅限于特定范围且使用人数很少,运营资质未必是强制要求(可能可采取本地备案或者提交合规性声明等低成本替代措施),建议具体咨询当地监管部门。
产品功能	1. 产品除提供入网使用外,是否支持用户间在线数据交互。	很多国家或地区对于支持在线数据交互功能的产品均有明确的电信资质要求。因此,如产品支持此类功能,存在申领相应电信牌照的较大可能性。在此基础上,应根据产品是否支持域外互联或者数据出境,关注所在国或地区对于纯本地运营及允许跨境的数据交互服务的不同牌照要求。
	2. 产品正常对外提供服务,是否需以在当地拥有独立电信网络运营,或者提供相应通话或网关服务为前置要求。	如是,则产品除了涉及增值电信业务外,还可能涉及本地基础电信服务,牌照要求会更加多样复杂。
技术特征	产品在网络运用(通讯网/互联网)、基站或服务器需求、无线射频谱使用等层面的具体指标特征。	部分国家或地区对于不同技术指标的产品,会有不同的电信牌照监管要求。

(2) 牌照申领

在明确落地所需的电信牌照后,需关注本地申领相应牌照的对应要求。除申请材料、办理时限、牌照有效期及续期安排等具体要求外,针对申领主体是否有注册国籍限制(即仅允许本国或本地区注册企业申领)、是否有独立法人身份(即不允许分公司、办事处等非独立法人实体进行申领)等要求,将直接影响出海企业在当地开展服务运营的主体选择。整体而言,目前主要国家或地区,针对非特定领域的一般性软件产品,在电信牌照申请管理层面,主要采取如下三类管理模式:

◆要求申领电信牌照的主体须为本国/地区注册的独立法人实体:例如泰国。

◆要求申领电信牌照的主体须为独立法人实体,但不要求必须为本国/地区注册法人:例如中国香港。

◆未限制申领电信牌照(或依要求无须申领牌照但需进行备案认证或提交合规声明)的法人主体性质:例如英国、法国、美国部分州(加利福尼亚州、纽约州等)。

建议出海企业在海外布局时,充分考虑对应国家或地区在牌照申领主体层面的条件限制情况,决定是否由本企业或由本企业另设/注资的法人实体进行相应申领工作,或者委托所在国或地区的本地电信运营商进行相应牌照申领及当地服务运营。

2. 产品认证

部分国家或地区,可能会对软件产品的安全认证,以及搭载相应软件产品的硬件终端的性能测试,进行强制性的前置要求。通常而言,如出海产品涉及如下特征,则一般情况下需重点关注落地国家或地区可能存在的、针对软硬件产品的测试认证要求:

- ◆产品涉及对码号资源、无线电频谱、卫星信号等的使用;
- ◆产品会在勘探、军工、海运等特定场合中予以投放使用;
- ◆产品存在电磁辐射等可能影响使用者身体健康的情形的。

对于经评估无需进行强制性测试认证的产品,为增强当地用户对产品的安全确信,方便产品在当地的顺利推广,建议运营企业可同步关注所在国或地区是否具备自愿认证申请的程序(例如泰国针对电信设备的供应商符合性声明制度),申请并张贴相应的认证标签。

另需注意的是,产品在境内已做过对应的CE认证、CCC认证等,一般情况下不能豁免这部分测试认证要求。

SECTION 002

数据合规

围绕个人信息保护的数据合规监管,是目前主要国家和地区加紧立法建设及执法检查的重点领域。主流国家及地区已建立或者逐步形成体系完善的数据保护制度,规制发生于本国境内的数据收集处理行为,或者通过服务提供方式收集、处理本国境内用户个人信息的场景。鉴于移动互联产品具有较强的用户交互特征,多数产品均将本地用户个人信息作为支撑服务正常运转的“源动力”,因此数据合规问题,属于互联网出海企业需高度重视的合规板块。

本部分将基于数据全生命周期管理理念,将多数国家及地区的数据合规的共性要求进行总结,从企业合规操作侧角度考虑,为出海企业合规提供通用的底线指引。

1. 个人信息收集处理规则/说明

个人信息收集处理规则/说明,常见形式为隐私政策,系产品运营者面向用户所公开的关于个人信息合规处理及保护的主要说明文件。因其内容集中性及公开性特征,也成为本地执法机关所重点关注的对象。一般而言,执法机关对于隐私政策的审查,主要基于以下方面及要点:

方面	
内容	<ul style="list-style-type: none">◆本产品运营者(数据控制者)的身份及联系方式;◆本产品涉及数据收集的功能场景、对应数据类型等,以及是否提示用户未征得其同意便可收集处理其个人信息的例外情形;◆自动收集工具(cookies等)的使用情况;◆用户数据存储地、存储期限,存储及传输等内部安全控制技术措施等;◆用户其个人信息可能用于市场营销、个性化推送等场景,并可随时撤回同意;◆个人信息共享的必要信息,包括数据接收方类型、共享目的、共享数据范围等;数据可能对外转让或者披露的情形说明;◆用户个人信息查阅、更正、删除、取得副本、撤回同意、注销账户等基本权利的实现方式;用户投诉、反馈的有效渠道,以及承诺回复时间;◆个人信息出境(如有)的必要信息,包括数据接收方类型及所在国、出境目的、数据范围等,以及为保障数据出境安全所采取的措施。
形式	<ul style="list-style-type: none">◆独立成文,具备本地语言版本;◆在用户首次使用/打开产品时,在界面中以显著标识(弹窗、内嵌链接等)方式提示用户阅读;◆以点击同意、勾选框设置等方式,获取用户对隐私政策的授权同意;◆如涉及大量cookies使用,可考虑单独设置cookies政策及提醒。

2. 第三方协议

基于产品本地部署安排,出海企业可能会就产品运营事宜,与本地或境外技术运维或者内容服务提供商、软硬件支持方等上游企业进行合作,也可能就产品实际推广及落地服务事宜,与代理商或者具体客户等下游单位签订合作协议。针对与上述上下游企业的合作协议的管理,尽管多数情况下本地执法机关不会具体审查协议内容,但就数据合规层面的责任义务约定,将影响产品本地服务的正常运营开展,以及一旦发生数据安全事件时的责任分配问题,对于预先保障出海企业的数据管理合法利益,追究他方的违约责任,具有关键意义。

为此,我们建议出海企业在处理与第三方的合作协议时,重点关注如下层面的条款;如存在条款缺失的,可通过补充签署数据处理协议等形式进行合规完善。

方面	要素
服务描述完备度	是否已具体描述其在特定服务场景(目的)下,合作方会提供或者可能访问的数据范围、类型、频率、数量等,以及提供或者访问的渠道、方式、时间段等。
数据来源合法性	合作方是否对其数据来源进行充分说明,或者对数据来源合法合规进行承诺。
对于提供的 数据的安全 管理责任	若合作中涉及向合作方提供数据的,应关注合作方是否对数据安全存储及处理、合作期限届满之后对该部分数据的处理措施(是否删除)、数据后续使用场景、数据安全保护、是否对第三方提供及保密义务承担、发生数据泄露等安全事件的通知及响应义务等方面,进行说明或者合规承诺。
服务或者成 果转售的限 制	合作方是否对其提供的服务或者成果在转售(含有偿转售及无偿提供)方面进行限制。如有,是否合理,是否会限制公司业务的正常开展或者承担相应的违约风险。
权利义务不 对等情形	在数据合规层面(尤其是面向用户)是否存在减轻供应商责任、不合理增加公司义务的相应条款。

3. 数据本地化和数据出境

针对数据本地化(即要求在境内收集处理的全部或特定类别的个人信息需在境内存储)及对数据出境的限制,实际上是各国或地区在网络空间主权、数据资源管控与数据流动带来的经济效益之间的权衡考虑。整体而言,目前主流国家或地区对此的管控举措,可分为如下三类:

(1) 明确要求数据本地化且对数据出境进行条件限制的

代表国家为俄罗斯。根据《俄罗斯联邦个人数据法》要求,运营商收集个人数据(包括使用互联网手段)时,需要保证使用位于俄罗斯境内的数据库,对俄罗斯公民的个人信息进行收集处理活动。对于此类国家或地

区,出海企业应严格按照本地法规要求,部署或者租赁本地数据库或服务器,做好数据本地化存储;如有必要进行数据出境处理的,遵照当地要求做好备案申报(行政措施层面,如有)、合作协议责任约定(民事责任层面)等应对措施。

(2) 不要求数据本地化但对数据出境进行条件限制的

代表国家或地区为接受欧盟《一般数据保护条例》(“GDPR”)管辖的国家及地区(主要为EEA欧洲经济区国家),以及在立法上借鉴GDPR模式进行数据立法的国家或地区(例如泰国)。这类国家或地区尚未明确要求数据本地化,允许数据有条件地向域外提供。一般而言,限制条件包括:数据接收方所在国或地区被数据共享方所在国或地区的数据监管部门认定为“具备充分保护水平”,则可无限制传输;通过企业的具有约束力的内部规则来约束和实现集团企业间的数据流动;与数据接收方签订数据处理协议,由数据接收方承诺按照合同履行其数据保护义务。鉴于中国目前的实践情况,对于此类国家或地区,建议通过内部个人信息安全影响评估流程(Data Protection Impact Assessment, “DPIA”),对数据出境的安全风险进行综合评估。经评估认定可推进数据出境的,通过与境外接收方签订数据处理协议的方式,厘清双方在数据出境合规及安全方面的责任义务。

(3) 目前对于数据本地化及数据出境未作过多限制的

此类模式包括两种情形:一是现有制度体系并未限制数据存储及出境(代表国家为美国);二是已制定了数据出境的相关限制要求但未生效(代表地区为中国香港)。在此类模式下,数据可在相关国家或地区自由流通。

4. 营销推送

营销推送,常以App内定向推送、营销短信、电话、邮件等形式呈现,系企业基于商业开发考虑所经常涉足的个人信息使用行为。因其与数据的经济价值直接相关,并直接影响用户的使用体验,容易引发用户投诉等情形,因此有不少国家或地区通过国内数据专项立法方式,对个人信息用于营销推送场景进行专门限制。综合来看,目前主流国家或地区,主要采用“opt-in”(以用户明示同意为推送服务开展前提)及“opt-out”(不以用户明示同意为前提,但需保障用户退出权利)的两种模式。两种模式的对应合规措施要求展示如下:

模式	Opt-in	Opt-out
代表国家或地区	接受GDPR管辖的国家或地区(主要为EEA欧洲经济区国家)、泰国、中国香港	美国
合规措施	<ul style="list-style-type: none"> ❖ 在隐私政策中说明该使用场景(目的、数据类型、具体场景信息) ❖ 隐私政策外设置单独提醒,并获取用户明示同意 ❖ 默认状态为关闭 ❖ 提供退出途径并保证退出机制有效 ❖ 退出后不会再打扰用户,并做好对应个人信息删除或者匿名化,或者至少不可被轻易获取和访问 	<ul style="list-style-type: none"> ❖ 在隐私政策中说明该使用场景(目的、数据类型、具体场景信息) ❖ 提供退出途径并保证退出机制有效 ❖ 退出后不会再打扰用户,并做好对应个人信息删除或者匿名化,或者至少不可被轻易获取和访问

5. 个人信息主体行权

个人信息主体的权利保障,同样是目前不少国家或地区数据合规监管的重点关注对象。综合相关立法及执法情况来看,尽管各国或地区对于个人信息主体所拥有的权利内容存在差异,但在监管直接关注的用户必要权利、展现形式及内部响应机制方面,存在一定的共通性。我们理解,出海企业应尽量保证自身产品能够满足如下共通要求,在此基础上关注具体法域在用户权利内容方面的进一步要求。

◆**必要权利内容:**个人信息查看、更正、删除的权利;撤回同意;获取个人信息副本;注销账户;投诉及反馈意见并获得积极响应。

◆**展现形式:**支持用户通过移动互联产品界面实现上述权利;对于难以实现或者需要进一步验证的,可支持通过预留的联系方式实现。

◆**内部响应机制:**出海企业内部应建立一套自用户反馈信息收集、转移至对应处理部门、及时处理并反馈用户的响应机制;对外载明反馈处理时间(一般不超过30日)。

6. 数据内控管理机制

数据内控管理机制,包括数据合规专职机构及/或个人的设置、信息安全事件应急处理机制、数据安全管理制度体系等部分,尽管其更偏向后台管理,在直接监管风险上稍弱于上述其他层面,但作为组织管理的必要构成部分,其同样常见于主要国家及地区的数据保护立法中。

综合目前主要国家及地区对于数据内控管理机制的建设要求,我们理解,在合规应对层面,应至少满足如下要求,作为整体数据合规处理的有效制度支撑。

◆ **专职机构及/或个人设置**: 出海企业应保证内部已建立负责数据合规事宜的专职机构(实体部门或者虚拟小组均可), 能够实际处理内部数据合规日常咨询、用户行权请求处理及投诉应对、隐私政策及第三方数据处理协议的审阅及更新等工作。

◆ **信息安全事件应急处理机制**: 出海企业应保证内部已搭建针对传统信息安全事件(安全漏洞、木马病毒攻击、数据泄露等)及个人信息安全事件(非法提供、个人信息大规模泄露等)的应急处理机制和预案; 机制和预案应覆盖自事件发现、处理、上报、用户告知至后续总结及培训提升等全流程; 保证日常有相应培训及演练活动。

◆ **数据安全管理制度体系**: 出海企业应在申请办理ISO /IEC 27001 信息安全管理体系认证的基础上, 参考ISO/IEC 27002及ISO/IEC 27701等关于个人信息合规处理及安全保护的最新国际标准的要求, 构建、完善内部数据安全管理制度体系。

SECTION 003

知识产权

1. 软件平台的风险和对策

移动互联网的软件产品, 如APP等, 基本上都依托于iOS或者安卓等操作系统的软件平台(以下简称为“平台”)上架销售。在实践层面, 平台在与企业沟通时一般都相对强势。面对可能发生的知识产权风险, 平台一贯秉持谨慎态度, 以免除自身责任为优先原则。而平台的这种态度, 却往往导致“一刀切”的下架行为。即平台一旦接到软件可能涉嫌侵权的投诉, 在双方长期争执不下时, 可能会优先考虑下架“侵权产品”以迅速争取善意免责, 往往忽视了针对侵权行为本身的分析判断。这种情况下, 移动互联网产品可能因竞争对手的“恶意”投诉而被迫下架。

以iOS平台为例, 权利人在平台投诉的程序非常简单, 只需在苹果官网的“App Store Content Dispute”页面填写权利人姓名、涉嫌侵权软件的链接等基本信息, 并简单描述争议问题, 平台就会将权利人的联系方式、争议内容发送给被投诉软件的开发商, 要求双方直接沟通解决争议。由于投诉程序简便, 并且iOS平台本身不会轻易针对侵权做出评判, 国外竞争对手恶意投诉软件、导致国内企业软件面临下架风险的情形时有发生。

以曾处理的类似案件举例。一家中国软件企业在iOS平台面向海外用

在商标领域,最常见的法律风险出现在商标申请阶段。随着企业知识产权保护意识的增强,许多移动互联网企业在产品投入市场之前,就同时开始准备境内和境外商标的申请注册事宜。



户连续推出了几款广受欢迎的软件,下载量和销售量都很可观,并迅速攀升到同类软件下载排行榜的前列。该企业的海外竞争对手不断向iOS平台投诉,认为该企业软件产品侵犯了境外企业软件的知识产权。虽然双方软件的用户界面、显示效果等具有明显区别,但该海外企业持续致信iOS平台,要求iOS平台下架所谓的“侵权软件”。iOS平台接到投诉后,不会直接去判断事实和法律问题,而是将投诉内容、联系方式直接转发给中国企业,要求双方通过往来信函解决。所有信函均要抄送平台,平台会根据双方的往来确定责任,并进而决定是否采取下架的措施。

该企业之前并未有专业律师参与处理,导致对手投诉成功,平台下架其产品,导致巨额的损失。我们介入后,迅速对双方的软件进行了专业的比对和分析,并组成专业团队代为向iOS进行交涉与回复,最终取得了对方撤回投诉的结果。

本案带给我们的启示是,由于存在善意下架免责的原则,平台类似于居中裁判的角色,而双方的往来函件则像法庭上的主张和抗辩。平台往往会就往来信函所体现出的事实进行裁判,采取有关的“必要措施”。因此遇到平台投诉时,企业应对的积极程度以及专业程度则显得十分关键。出海企业需要有专门的预案和专业律师的支撑,才能最大限度的保护自身合法权益。

2. 商标和著作权保护的问题

1) 商标领域的常见法律风险

在商标领域,最常见的法律风险出现在商标申请阶段。随着企业知识产权保护意识的增强,许多移动互联网企业在产品投入市场之前,就同时开始准备境内和境外商标的申请注册事宜。许多企业认为,多数国家的商标申请流程相似,因此仅给出一套粗略的申请方案,就匆匆在各个国家提交了商标申请。这其中其实隐藏了重要的法律风险。事实上,每个国家的商标申请流程、所需文件、审查思路均有不同。在提交商标申请之前,如对当地法律实践缺少认识而匆匆提交申请,一方面可能会延误商标专用权的取得,另一方面企业在未来使用商标时可能会面临巨大的法律风险。

笔者以美国商标申请的实践为例,阐述中美商标申请的几点不同。首先,在中国,商标申请的提交流程比较简便,在提交商标申请时无需提供商标的使用证据。但在美国,如果商标申请不是以本国有效商标注册为基础的,那么在商标申请提交后短时间内,申请人就需要向美国专利商

标局提交商标的使用证据。其次,中美两国商标申请在挑选指定商品时的思路不同。在中国提交商标申请时,出于扩大保护范围的考虑,企业往往会倾向于多选几项指定商品,或者多选几个与产品有关系的类别。但在美国提交商标申请,出于实际使用意图的考虑,我们反而会建议客户尽量选择与其产品具有最密切联系的指定商品。否则,在美国商标申请的后续程序中,即“提交商标使用证据”时,美国专利商标局会要求企业删除与产品联系不紧密的商品。第三,很多企业在提交商标申请之前,都希望在目标国家或地区的官方商标数据库中检索近似在先商标,以判断商标注册的可能性。但各国商标数据库的更新情况各不相同,中美审查员的社会经验、文化均具有差异,即使检索出可能近似的在先商标,我们也不能使用中国业内判断商标近似的思路来直接推断美国商标的近似性。第四,如发现企业的商标在美国遭遇抢注,在清除抢注商标时,中美在程序方面和实体方面均有较大差异。特别是美国商标异议案件的流程、判断思路、证据收集方式,均不能直接套用中国商标异议案件的经验。因此,当跨境移动互联网产品涉及商标相关的问题时,我们建议企业邀请专业的商标律师介入,根据当地实践给出具体的法律意见,一方面更高效地规避在先近似商标带来的法律风险,另一方面如遇商标被抢注的情况,商标律师能够给出符合当地实践的、更可行的应对策略。

2) 著作权领域的常见法律风险

移动互联网企业的跨境产品中,有时部分画面、视频、角色设计等要素可能被域外主体主张侵犯他人著作权。许多域外企业在知识产权领域比较激进,可能会第一时间发出措辞强硬的律师函,或者要求平台立即下架中国企业的产品,对我国企业造成巨大的心理压力。但在实践中,许多行为是否真正构成“著作权侵权”实际上仍值得商榷。

首先,著作权法只保护“表达”,不保护“思想”,即“思想表达两分法”。以游戏软件为例,一家企业无法垄断一种游戏的玩法,因此不可能禁止他人使用不同的游戏画面组织同一种游戏玩法。例如,A公司拥有一款消除类游戏“宝石消除”,核心玩法是,玩家通过移动方格中的“宝石”,将三个或者更多的“宝石”连在一起,即完成消除,消除的宝石越多、越快,得分越高。B公司之后也推出一款相同玩法的消除类游戏“糖果连连”,玩家通过移动方格中的“糖果”,将三个或者更多的“糖果”连接,即完成消除。此外,“糖果连连”游戏中还设置了可以成片、成条地消除糖果的特殊道具,以及为游戏增添难度的、不易消除的特殊糖果。B公司的游戏“糖果连连”虽然在核心玩法上与A公司的“宝石消除”完全相同,但游戏画面、细

节设置、事件触发后的动画效果、奖励机制等方面相差迥异。如A公司主张B公司的游戏侵犯了A公司的著作权,那么依据“思想表达两分法”,我们认为A公司的主张恐难成立。

另一方面,即使作品的部分内容确实涉嫌侵权,专业的知识产权律师能够针对涉嫌侵权的部分给出修改建议,提前规避侵权风险。

著作权侵权的考量因素相对复杂。不同法域中对侵权的判断因素各不相同。移动互联网企业如在跨境经营时遭遇他人主张著作权侵权,建议不要对对方律师函等法律文书置之不理,更不要贸然自行回复。企业应当委托专业的知识产权律师研究案情,分析获胜的可能性,并根据当地法律实践制定合理的应对策略,从而更好地维护自己的合法权利。

SECTION 004

总结

《礼记·中庸》：“凡事豫则立，不豫则废”。法律基于其地域性、多样性等特点，即使是同一种法律体系下的同一项制度，在实施执行层面仍会有千差万别。出海企业在关键产品和服务出境之前，应当做好功课，梳理形成通用、精炼的对策清单，提前识别核心风险；出海后如遇到法律纠纷，应当以积极的心态应对，建立本地化思维，找到最优解决方案。

Facebook与美国联邦贸易委员会就剑桥分析丑闻达成的50亿美元和解协议就充分说明了企业在海外经营应当重视内部风控制度的建立和信息安全事件应急预案。对于出海企业而言，合规工作尽量避免“解渴”心态，而需要“未雨绸缪”的规划和“一以贯之”的决心。



蔡鹏/合伙人
知识产权部
北京办公室
+86 10 5087 2786
caipeng@zhonglun.com

总编辑

陈际红

张炯

龚乐凡

编委 (按姓氏笔画排序)

丁恒

朱永春

邱建

周月萍

周兰萍

周洋

蒋蕙匡

蔡鹏

樊晓娟

薛熠

特别声明：以上所刊登的文章仅代表作者本人观点，不代表北京市中伦律师事务所或其律师出具的任何形式之法律意见或建议。未经本所书面授权，不得转载或使用该等文章中的任何内容，含图片、影像等试听资料。如您有意就相关议题进一步交流或探讨，欢迎与本所联系。



中倫律師事務所
ZHONG LUN LAW FIRM



中倫研究院出品