中倫律師事務所
ZHONG LUN LAW FIRM

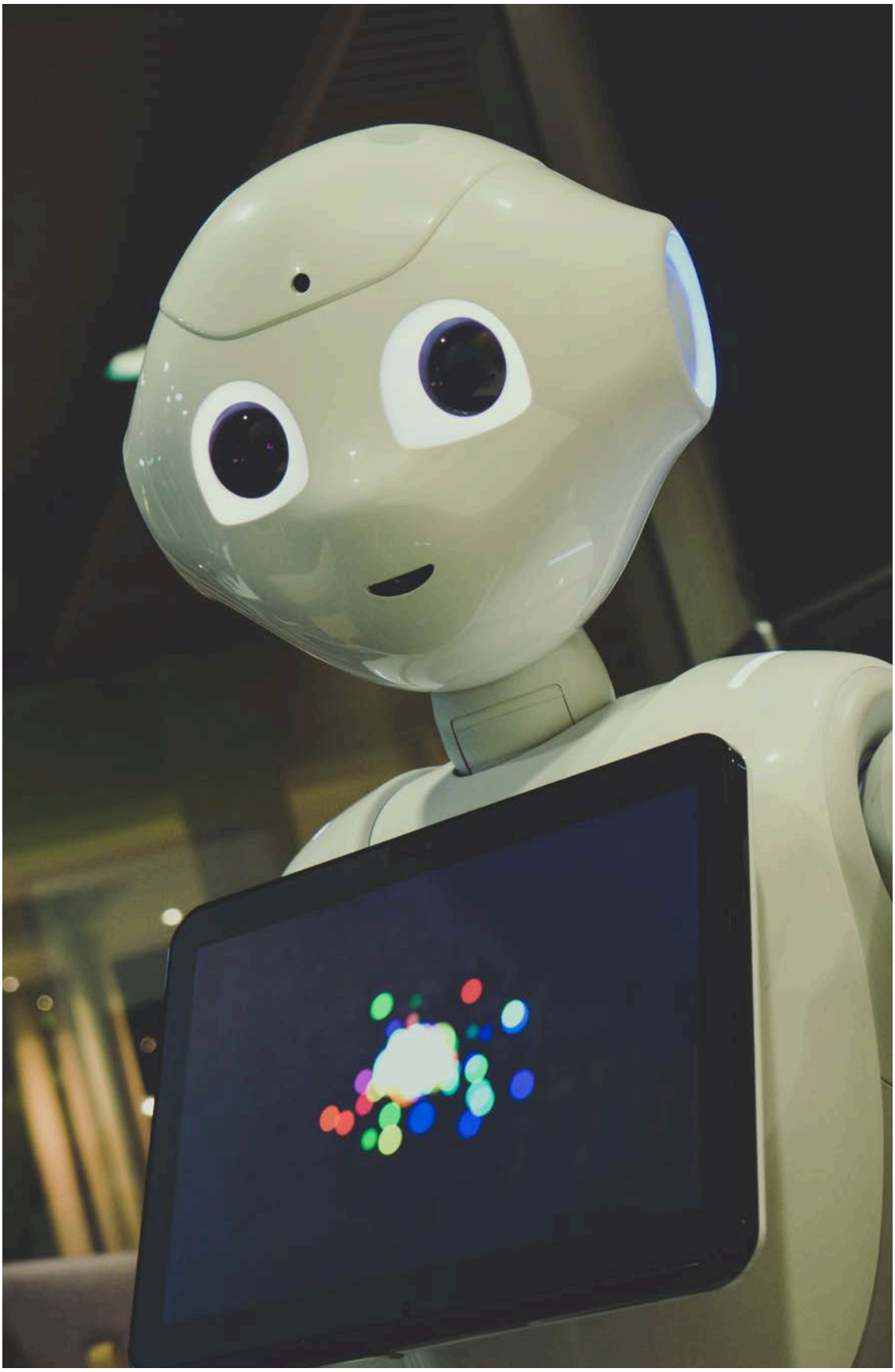
人工智能

知识产权保护和数据合规

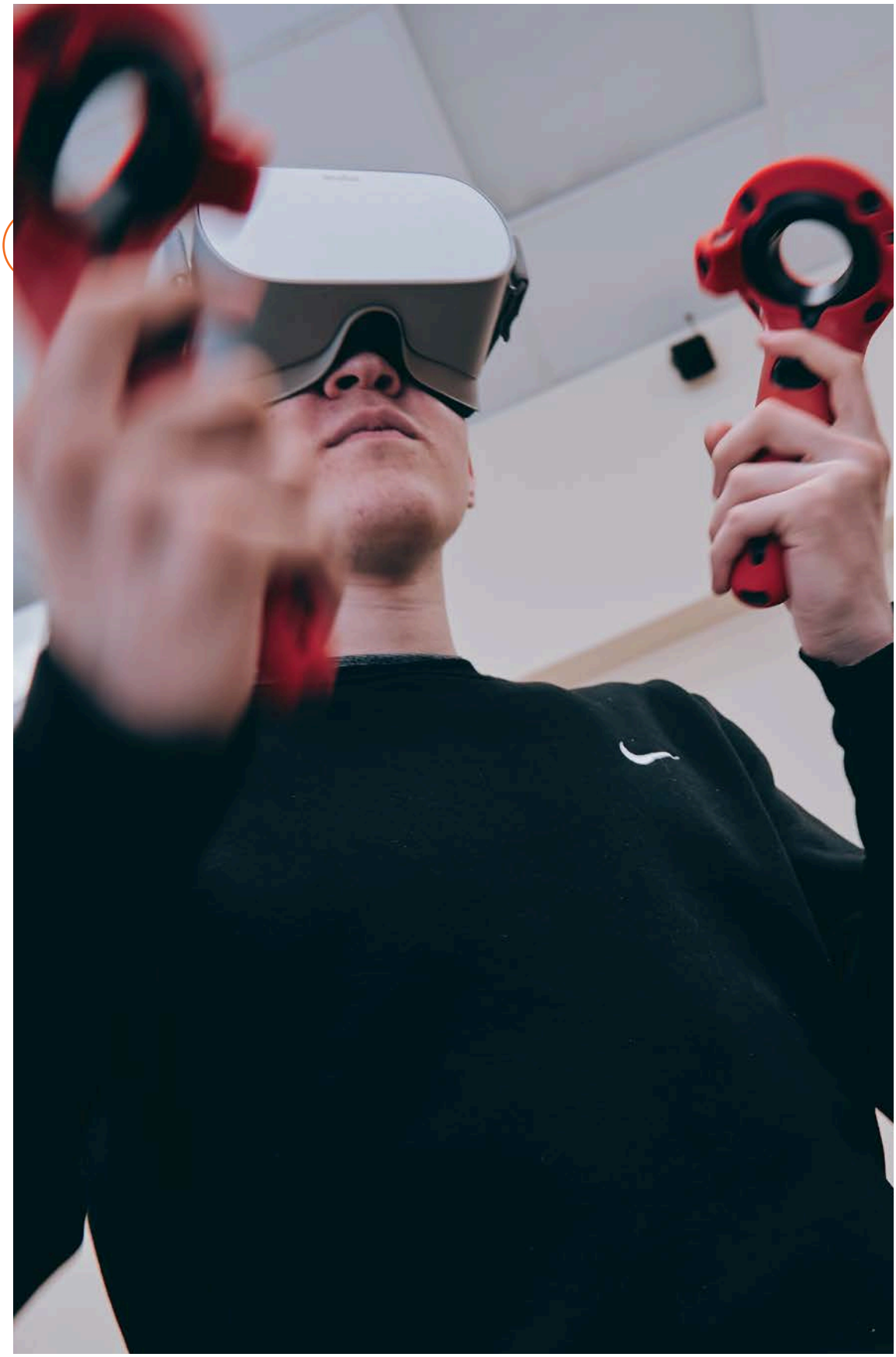
ARTIFICIAL INTELLIGENCE:
INTELLECTUAL PROPERTY
PROTECTION AND
DATA COMPLIANCE

中伦研究院出品

CONTENTS



CONTENTS



PREFACE

2021世界人工智能大会于7月8日在上海开幕，与基因工程技术、纳米技术并称为21世纪三大尖端技术，人工智能这门关于模拟、延伸、扩展人的智能的技术科学已然走到了我们身边。国际数据公司（IDC）与浪潮集团日前联合发布的《2020-2021中国人工智能计算力发展评估报告》预测，2024年，中国在全球人工智能市场的占比将达到15.6%，成为全球市场增长的重要驱动力。报告预测，中国人工智能市场未来4年将保持30.4%的年复合增长率，2024年将达到172.2亿美元的市场规模。

1.澎湃新闻：全国人工智能行业十年融资额达3万亿元！《人工智能（2010-2021）行业发展研究报告》发布https://m.thepaper.cn/baijiahao_13630136（最后访问日期2021年7月23日）

人还是人工智能？

对于人工智能来说，2020年足以载入“史册”。截至2021年4月30日，人工智能产业处在申请中的发明专利共计934185件，已授权发明专利共354150件，产业发明专利（含授权和申请）占比高达65%。[1]我国人工智能发明专利授权总量全球排名第一。

在全球抗疫的背景下，人工智能技术深度参与了医疗、基础建设、城市治理、教育、制造、无接触服务等领域，助力各产业环节。人工智能正在进入技术与产业交融发展的阶段，新一轮的技术革命在不断革新社会面貌的同时，也不可避免地会对传统知识产权保护体系带来巨大冲击。

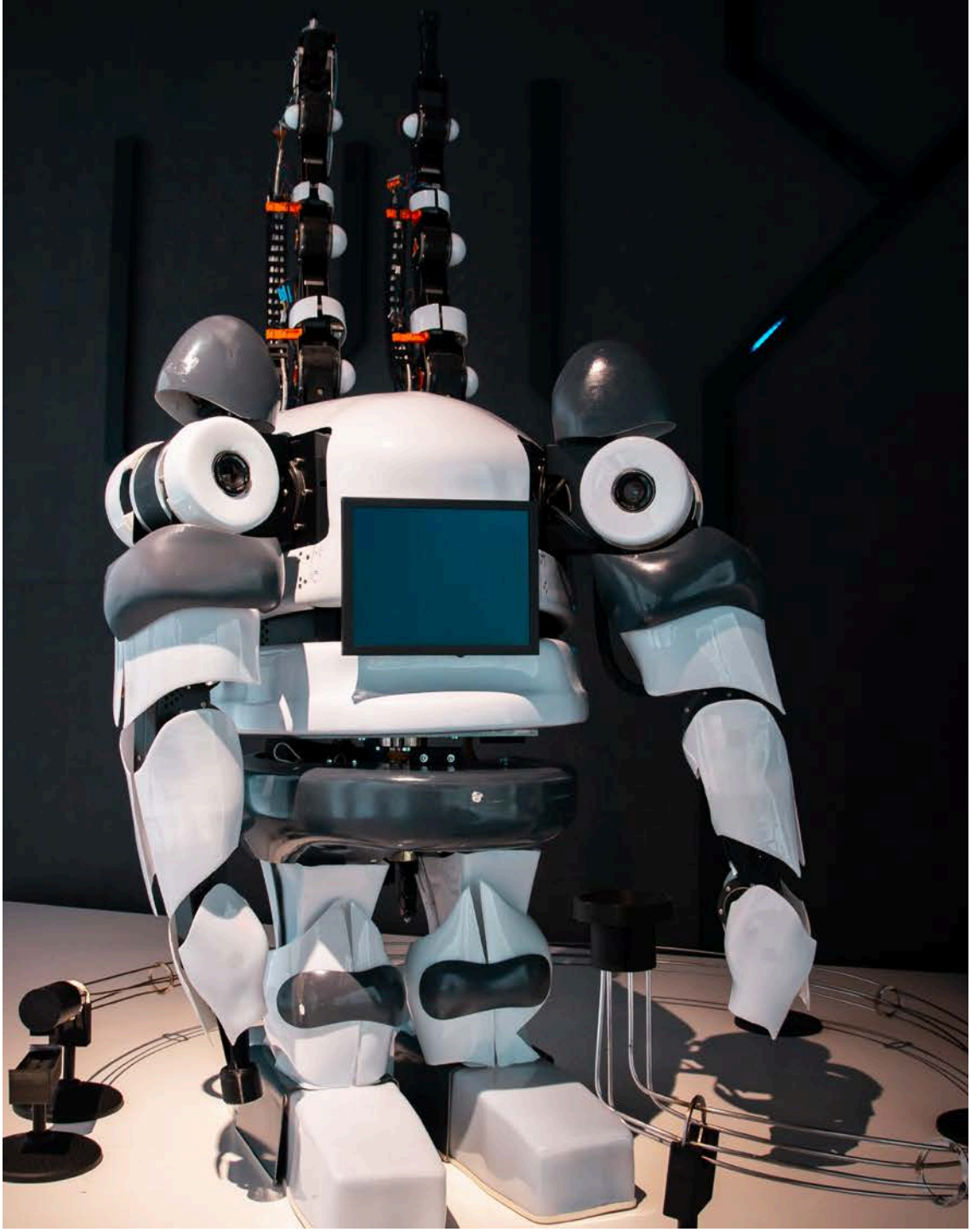
“法的人格者等于权利能力者。”当人工智能的生成物愈发接近人类的创造，智力创造成果不再是人类的专属，在知识产权法律关系中，人工智能能否通过智力劳动被视为“作者”、“发明人”？人工智能生成发明是否具有可版权性、可专利性？ 在知识产权法律实践中，人工智能企业如何应对潜在侵权风险，布局知识产权管理体系？围绕着人工智能的学理法理之争论和监管边界正因法律人的努力探索而不断被厘清。

数据风险与隐私保护

人工智能无法离开数据这个核心要素。大数据时代下，人工智能的研发和运用周期，同时也是数据全生命周期（收集、存储、使用、共享）的周期。作为新时代人工智能企业发展的石油，数据对于人工智能行业发展而言，有着基础资源和助推动能的作用。

迎接数字时代，激活数据要素潜能。在促进数字技术发展、鼓励企业数字化转型、建设重点行业人工智能数据集，推进人工智能“云端”落地的同时，世界各国纷纷出台相应政策监管法律法规，应对AI技术滥用、隐私泄密、数据投毒、数据流通及共享安全等难题。伴随着《网络安全法》和《数据安全法》的出台，以及不久将顺利通过的《个人信息保护法》，我国网络空间监管和数据保护的基本格局即将成型。“十四五”期间，国家也将大力构建起与数字经济发展相适应的政策法规体系，为人工智能的发展完善监管框架，提供肥沃的土壤。

创新为面向前沿发展的第一驱动力，产业新趋势的背后，机遇与挑战同在，利好与风险并存，发展与监管并重。《中伦法律文集之人工智能知识产权保护与数据合规》布局大健康、金融科技、自动驾驶等热门行业，聚焦知识产权许可、商业秘密管理、科创板上市、出口管制、专利争议解决等核心法律问题，以期助力企业客户共同挖掘人工智能产业的巨大潜力，助力构建合法合规安全可靠的行业体系，助力数字中国蓬勃发展！

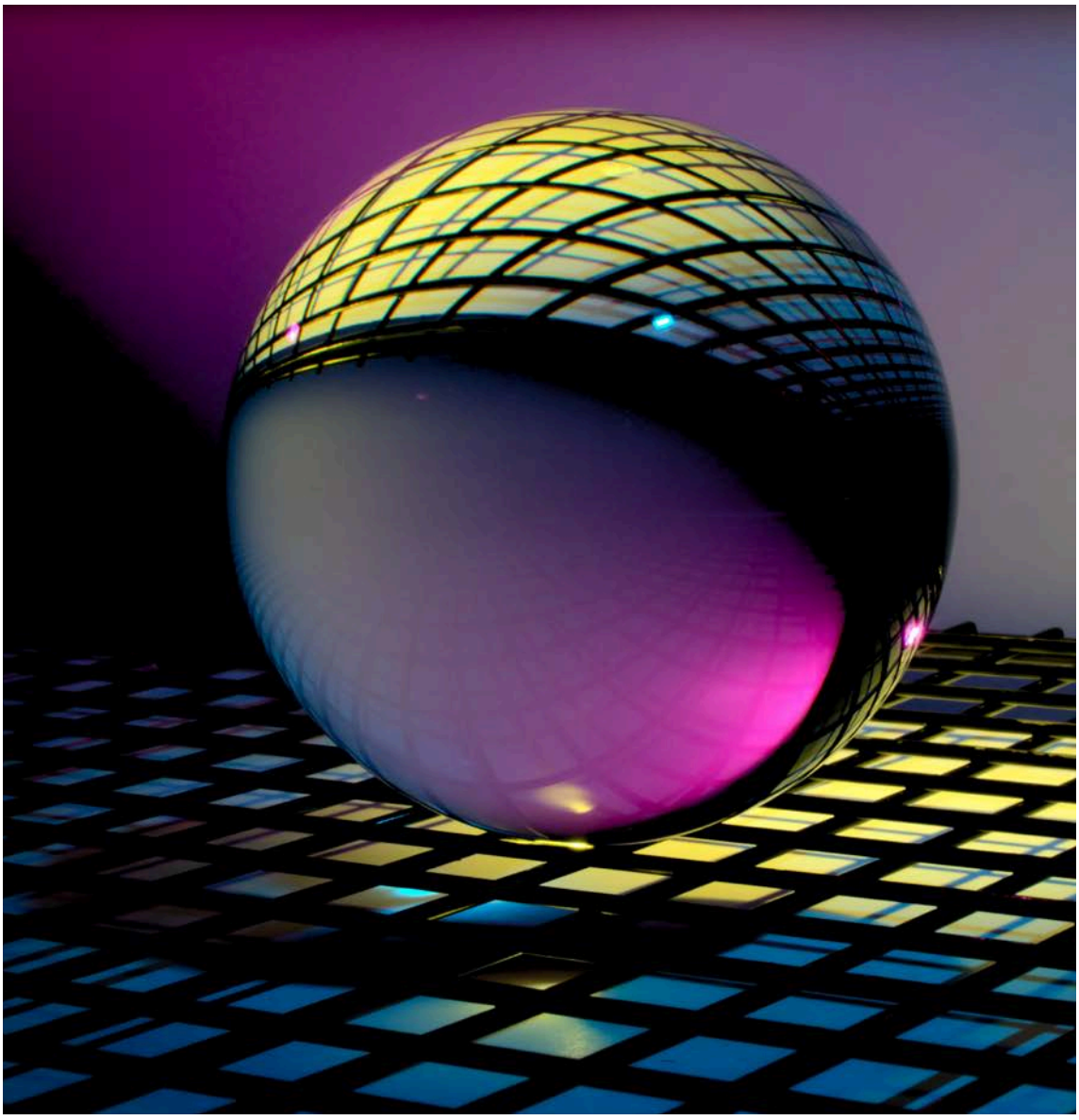


CHAPTER

1

人工智能领域的知识产权保护热点

HOT SPOTS OF
INTELLECTUAL PROPERTY PROTECTION
IN ARTIFICIAL INTELLIGENCE



人工智能技术与开源软件

作者/王红燕、徐琳

2021年5月，中国新一代人工智能发展战略研究院在第五届世界智能大会上发布《中国新一代人工智能科技产业发展报告•2021》。报告显示，2020年度中国的人工智能科技产业发展势头强劲，在新冠疫情的冲击下，进一步刺激了社会对产业智能化的潜在需求，人工智能已经成为新一代产业改革的核心驱动力。

时间往前倒回上个世纪50年代，早期的人工智能还只是一个设想，英国数学家、逻辑学家图灵在提出一项关于检测机器是否具备人类智能的猜想，即让被测试者（人）向人与机器询问问题，如30%以上的被测试人无法分辨做出回答的是人还是机器，即说明该机器具备了像人一样的思考能力。这是最早对人工智能概念进行解释的观点之一，同时也为后来的人工智能技术的研发奠定了基础。1956年，计算机专家约翰•麦卡锡提出了“人工智能”一词，主要是指利用计算机技术模仿人类思维的工具，这也被人们认为是人工智能正式诞生的标志。在这之后的几十年时间里，计算机技术的发展使得机器人、语言识别、图像识别、自然语言处理等技术获得了突发猛进的进步，人工智能时代的开启越来越近。

然而，人工智能技术发展的同时也带来了诸多社会问题，例如部分工种逐渐因技术的进步而消失、造成了社会失业人群比例上浮；不平等、不知情的机器操控等情况。2021年4月21日，为促进欧盟地区人工智能技术的使用、投资和创新，欧盟委员会通过了《人工智能法》提案，旨在建立关于人工智能技术的统一规则。根据欧盟委员会的定义，人工智能技术是指采用官方所列明的一种或多种技术和方法开发的软件，并且能够针对特定人群或具体目标产生诸如内容、预测、建议或决定等一系列影响其交互环境的输出技术。提案将人工智能技术可能存在的风险划分为不可接受的风险、高风险、有限的风险和极小的风险，希望通过有效的监督措施推动人工智能技术的良性发展。

PART 01
开源软件对人工智能技术发展的影响

人工智能技术的发展离不开基础研究的深入，这一技术的发展非常迅速，科技巨头们都在着眼于构建具有活力的开源社区，以便拓展自身的开源生态圈。2015年，谷歌推出了其开源框架解决方案TensorFlow，它是一个用于机器智能的开源软件库，吸引了不同的企业到这个平台训练他们的模型，

这个系统的通用性使其也可广泛用于其他计算领域。Facebook也推出了Caffe2框架，旨在让微软和亚马逊等主要市场参与者和社交网络的PyTorch框架一起使用这个平台。[1]开源平台的发展确实让企业获得了更多创新力量，他们推出的深度学习开源平台在全球人工智能领域占有很大的份额。截至目前，知名开源社区GitHub上已经汇集了6500多万的开发者、300多万家公司和机构，汇集超过2亿的代码库，其中人工智能项目的占比很高，人工智能代码开源已经成为了发展的主要趋势之一。[2]2021年7月8日，中国科学院院士梅宏在世界人工智能大会上提出，人工智能的快速发展离不开代码开源和数据开放，高质量的开放数据促进了深度学习算法突飞猛进，深度学习框架极大提升了算法开发的效率，两者相辅相成。[3]

在大数据产品领域中，基本上所有的数据库产品都绕不过使用MariaDB、PostgreSQL和MongoDB等开源数据库的核心代码。著名手机系统安卓系统也采用了Linux内核项目，而该项目本身也是开源软件。开源软件的运用使得其他使用者不用从头开始开发一个全新的系统，只需要在已有的开源项目的基础上进行修改和定制即可，最重要的是，开源软件通常是免费的，这在很大程度上刺激了行业创新的积极性。

我国的人工智能开源项目正处于起步阶段，2018年中国人工智能开源软件发展联盟发布的《中国人工智能开源软件发展白皮书（2018）》中指出，人工智能开源软件是驱动人工智能技术创新和应用的重要支撑力量。2021年两会期间发布的《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》中也指出，“支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。”目前，我国已经构建了OpenI启智平台、之江天枢人工智能开源平台等项目，为人工智能行业的发展提供新动力。

PART 02

开源软件的特点

1.什么是开源软件？

开源软件对人工智能技术的发展至关重要，那么了解开源软件的法律性质就成为使用开源软件的前提。开源软件通常被认为是指开放源代码的软件，任何人可以查看、修改或者增加其源代码。开源软件与专有软件不同，专有软件的使用需要经过作者的同意或者获得授权，一般情况下还需要支付费用。而开源软件是由其作者将源代码公开在网络上，任何人可依据开源

1.参考链接：https://cloud.tencent.com/developer/article/1051255,《格局可能会改变?科技巨头们正在使用开源框架来主导人工智能社区》

2.参考链接：http://www.xinhuanet.com/tech/2019-10/17/c_1125114032.htm,《开源开放是人工智能发展主要趋势之一》

3.参考链接：https://finance.sina.com.cn/tech/2021-07-08/doc-ikqciyzk4243170.shtml

协议的要求使用相应的源代码。开源软件仍然属于作品，受到著作权的保护，开源软件的作者仍然对其公开的源代码享有著作权。需要明确的是，在没有任何前提地公开源代码并不意味着任何人可以随意使用，相反，根据各国著作权法一般的规定，著作权人对源代码享有权利，任何人不得未经同意复制、使用、传播其作品。因此，如果作者希望更多的人能够来使用、修改、完善自己发布的代码，其可以通过选择相应的开源协议，通过建立作者与使用者之间的授权许可关系，免除使用者的侵权责任。

4．参考链接：https://www.sohu-.com/a/201032826_261288

2.与开源软件有关的机构

既然开源协议对使用者的行为提出了相应的要求，那么又由谁来保证使用者实际遵循了这些要求呢?1985年，理查德•斯托曼发起成立了自由软件基金会（Free Software Foundation，**FSF**），它是一个致力于促进计算机用户自由的非营利组织。最初成立该组织的目的是为了促进自由软件的开发，目前该协会自身就拥有GNU操作系统的版权。除此之外，通过协议签署，FSF已经拥有大多数GNU软件和其他一些自由软件的版权，以便FSF可以通过诉讼要求使用者履行开源协议项下的义务。

早在2008年，思科公司曾因为其销售的无线路由器Linksys WRT54G的固件中使用了GNU/Linux系统但未向用户发布所有的源代码而遭到FSF的起诉。在此之前的几年中，FSF一直尝试与思科公司沟通希望说服其主动发布产品源代码，但是并没有得到有效的回复。在诉讼过程中，双方最终达成和解，思科公司将任命一名免费软件总监，负责使Linksys品牌产品符合GPL授权方式，并向FSF汇报相关情况。思科公司还将告知现有Linksys客户他们的权利，并在网站上发布产品源代码，将源代码反馈给FSF。

除了拥有开源软件版权的机构，开源软件的作者自身也可以依据开源协议的内容进行维权。德国的Netfilter内核子系统贡献者Patrick McHardy就曾以不遵守GPL为由，自行担负起GPL执法角色，联络了德国的许多企业索要小额金钱，在18个月内他利用这种方法“索取”了200万欧元的收入。然而据报道，相关行业的专家在评估了Patrick McHardy对Netfilter内核子系统的贡献之后，认为其对整个系统的贡献有限，只能就其所创作的作品享有权利，而不能就整个项目主张版权。因此，社区维权被认为是更理想的维权方式，不过在开源社区中，大多数人认为更主要的努力方向是促使使用人合规，而不是惩罚。[4]

3.开源协议主要类型

(1)开源协议的主要内容

开源协议是软件开源时使用了许可证,其主要作用是规定了许可内容,以便使用人能够自由地使用作者发布的源代码,而不必担心侵权他人版权的问题。一般的软件许可协议中会规定许可使用的期间、地域范围,权利类型,许可的具体权利,如复制、修改、传播、收费等权利。我国的《著作权法》规定著作权人有16项基本权利以及1项其他权利。某些开源协议中还会对代码有关的专利许可进行约定。

(2)常见的开源协议

目前比较常用的开源协议有GNU General Public License (**GPL**)、Apache License 2.0、BSD licenses、“Lesser” General Public License (**LGPL**)、MIT license、Mozilla Public License 1.1 (**MPL**)和Common Public License 1.0等,已有的开源协议已经多达八十几种。

GPL是由自由软件基金会发行的用于计算机软件的许可证。目前大多数的GNU程序和超过半数的自由软件使用此许可证,知名的Linux就是采用了GPL。GPL允许代码的免费使用和引用、修改,并且要求修改后和衍生的代码做为闭源的商业软件发布和销售。这就导致任何基于GPL许可证项下代码修改的衍生产品在向公众提供时的同时需要公开其源代码。支持者认为GPL保证了代码自由的延续,任何基于前人智力成果创作的新产物也必须向公众免费公开;而反对者则认为,GPL的强制开源要求会导致企业不再愿意选择为GPL的开源代码的创新做贡献,因为他们不愿意将自己的衍生产品开源。

LGPL直译是更少限制的GPL,它允许衍生产品作为闭源产品,这也是考虑到私有软件闭源的需求,促进开源软件的应用和推广。这也是使用GPL发布的开源软件风险度较高的原因所在,绝大多数诉讼都是由于企业未能发布应用GPL开源软件衍生品的源代码而引发的。

Apache License 2.0是非盈利开源组织Apache采用的协议,其允许代码修改,再发布,且不需要强制衍生产品的开源。但是如果修改了代码,需要在被修改的文件中说明。在衍生产品中需要包括原来代码中的协议、商标、专利声明和其他原来作者规定需要包含的说明。Apache License对于商业应用来说是较为友好的许可类型,使用者可以修改代码并作为自己的商业产品进行销售。

MIT许可证是更为宽松的许可证类型,使用者可以使用、复制、修改软

件，并且将其作为商业软件发布，MIT唯一的限制就是在软件和软件的所有副本中必须包含版权声明和MIT许可声明。

PART 03

使用开源软件的主要风险

1.开源协议的法律风险

在开源协议的背景下，选择适合企业情况的许可证至关重要。这决定了软件使用者的自由程度。如果选择得当，企业可以享受开源社区便利的同时提高自身产品的适应性。但是选择不当，则有可能为衍生产品的使用埋下隐患。

（1）GPL许可中的强制开源

GPL协议具有高度的“传染性”，其允许第三方对开源的代码进行免费使用、修改，但是不允许将修改后的代码作为闭源的商业软件发布和销售。著名的Linux内核开源项目就是使用的GPL协议，由于使用Linux内核开源项目的上层服务不可避免地会涉及到调用Linux内核的文件，如果将该行为视为创作了衍生产品，那么将导致上层服务的源代码将会被受GPL协议控制的Linux内核开源项目所“传染”，从而需要接受GPL协议。这就形成了一个以Linux内核开源项目为核心的传染源，任何基于Linux开发的内核到驱动到中间服务到上层应用都受到GPL协议的控制，在符合发布软件的条件下需要向大众开放源码。不过Linux内核的作者Linus Torvalds以及内核开发人员多次澄清普通系统调用为非GPL的作用范围，也就是允许Linux用户空间的程序使用其他许可证。

2018年，软件自由保护协会（Software Freedom Conservancy）罕见地在其博客对某知名车企的GPL合规问题的细节进行了披露。SFC指出，其从2013年6月以来就收到多起有关S车型的GPL违规报告，该车型搭载的车载系统中含有BusyBox和Linux项目，但是该公司却迟迟没有向用户公开该系统的源码。SFC就此问题一直在督促其尽快提供完整的，但是在漫长的沟通过程中，该公司至今仍然没有向SFC或者公众提供符合GPL协议要求的源码。

Android系统中也包含Linux内核程序，由于Linux内核程序遵循的是GPL v2许可证，而GPL v2与其他许可证并不兼容，这就导致就算Android其他部分使用的是不要求发布源代码的许可证，也不能阻碍Linux内核程序的作者要求使用者遵循GPL v2协议的发布规则。但是Android系统构建

5．参考链接：https://www.synopsys.com/blogs/software-security/software-licensing-decisions-consider-dual-licensing/

了一种特殊的结构，其上层服务多使用了Apache 2.0许可证，它允许使用人对修改后的代码闭源。基于前述Linux内核程序认可系统调用类型的使用不属于衍生作品的范围，只要将使用方式限定于系统调用就可以免受GPL协议传染性的影响了。因此Android系统内在内核中构建了一个影子驱动，仅具有传输控制命令和数据的功能，而需要保护的源码则放在HAL层，以二进制包的方式发布。Android的发布方式为想要商业化使用Linux内核的企业提供了参考，但是该方式目前在实践中也存在争议。

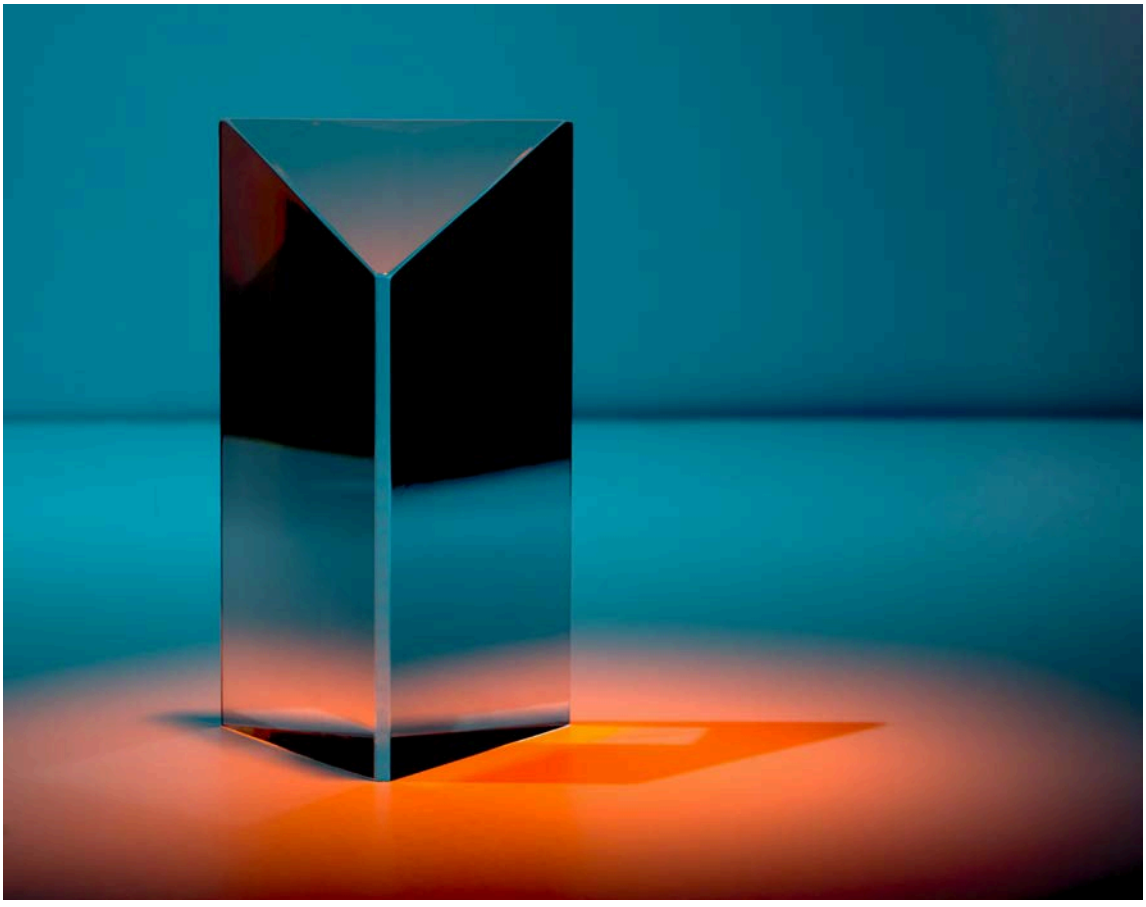
另一个值得注意的点是，GPL协议要求使用者在分发软件时提供源代码，这意味着如果使用者在修改代码后不以分发的方式向用户提供程序，那么就没有必要向用户提供代码。例如目前Saas模式下，供应商将应用软件部署在自己的服务器上，用户通过互联网获得供应商提供的服务，而不需要供应商发布任何的源码或者目标代码。在这种情况下，供应商不存在代码发布行为，因此不需要将修改后的代码予以开源。

(2) 双重许可

双重许可是指版权方既把产品作为商业软件销售，又适用开源协议供公众使用。一方面，版权方可以通过商业销售获得利润，另一方面，又可以利用开源社区的优势为软件更新增添活力。例如许可人可以选择同时使用专有许可和GPL协议，GPL协议保证了被许可人如果要发布修改后的产品，其必须一并提供产品的源代码。当然许可人也可以选择更为宽松的许可证，这样可以利用开源社区强大的研发力量更新自己的产品，将衍生代码合并到自己的产品中。MySQL数据库管理系统使用的就是双重许可的模式，一边以专有许可的模式满足用户的使用需求，一边以GPL许可证的优势来获得更新的软件。在Artifex Software, Inc.（“**Artifex**”）和Hancom, Inc.（“**Hancom**”）之间的诉讼中，Artifex发布了Ghostscript，并同时以专有许可和GPL许可的方式授权第三方使用，其诉称Hancom未能遵守GPL许可下的义务，在免费使用Ghostscript的情况下，将其修改的版本整合到自己名为Hangul的商业软件中对外销售产品，但是没有分发产品的源代码。[5]

(3) 违反开源协议后的法律风险

欧洲自由软件基金会的FTF部门与GPL维护组织（GPL-Violations.org）在2008年发布了一份《举报和修复违反许可证行为指南》，该指南主要是对常见的开源软件合规性问题进行解释。例如任何人都可以向基金会或者GPL维护组织举报企业的违规行为，当收到举报通知之后，欧洲自由软件基金会与GPL-Violations.org会通过邮件或信件方式与违规者协商，协商不成可能会采取诉讼方式达成庭外和解或者申请法院禁令。根据



GPL-Violations.org的经验，其已在德国和美国获得了成功的案件判决。

2.专利侵权的法律风险

开源软件仅是就软件授予著作权方面的许可，在某些开源协议项下并不包含专利许可，因此如果软件包含已申请的专利，使用该开源软件就有可能存在专利侵权的风险。例如，BSD、MIT许可证就不包括专利许可，而Apache-2.0和GPL协议则包含了专利的普通授权许可，使用人在获得著作权许可的同时也不必担心存在专利侵权的风险。对于没有明示有专利授权的开源软件，在使用前应当进行相关的专利检索，如存在有效的专利，使用该开源软件则存在专利侵权的风险。

6．参考链接：https://www.freebuf.com/articles/-paper/186281.html

7．参考链接：https://www.sohu-.com/a/407098658_675634

3.软件漏洞的法律风险

在使用开源软件时，一旦开源软件的代码存在安全缺陷，人工智能企业将面临着严重的安全问题。据调查，针对人工智能行业在开源软件代码安全缺陷分析中，项目主要的安全缺陷就来自于API误用和代码质量问题，其比例占所有安全问题的94%。[6]而使用开源软件因其缺陷问题受到网络攻击的后果只能由使用者自行承担，无法向开源软件的提供者进行追偿。例如RealAI发布的RealSafe人工智能安全平台通过测试得出某些云服务的人脸比对演示平台存在巨大安全漏洞。目前，人脸识别技术广泛应用于金融远程开户、手机解锁、支付验证等场景，如果这一漏洞被不法分子所利用，将会对用户的人身财产安全造成巨大影响，届时可能会产生用户向产品供应商进行索赔的情况。

4.出口管制的法律风险

随着中美关系的日益紧张，美国对中国实行的技术进出口管制政策趋于严厉，美国联邦政府发布的《出口管理条例》（Export Administration Regulations，以下简称“**EAR**”）不但可以管制从美国境内向境外输送实物产品，还包括向美国境外人员提供用于电子传输的软件。在全球最大的代码托管平台Github的用户协议上明确表示，其网站上的信息都可能受美国出口管制法律的约束，包括美国出口管理条例（EAR）。Apache基金会开发的产品是通过公开论坛在线协作完成的，通过美国的中心服务器进行分发，因此Apache开源协议也同样需要受到美国出口法律法规的管辖。

不过，根据EAR的规定，大部分已发布的开源代码并不会受到进出口的限制。例如，已公开发布的开源软件、已公开发布的开源规范、已公开发布的，说明硬件设计的开源文档和已公开发布的开源软件二进制均不受EAR的限制。但是，EAR规制了特定加密软件和技术的出口，包括仅激活或启用其他软硬件产品的加密功能的软件。[7]因此，在使用开源软件时还应当结合当地的技术进出口管制措施，如相关技术落入管制范围，则需要按照当地的法律法规进行申报获得许可后才能引入，否则可能引发不必要的法律风险。

PART 04
人工智能企业合规建议

1.开源软件管理审核

为避免在使用开源软件过程中发生的风险，建议企业在内部管理机制

上增设开源项目管理流程或者部门，以便对开源软件的使用安全性、合法性进行评估。随着国际化程度的不断加深，中国产品越来越多出口到国外，开源软件风险问题也日益突出。企业可能会遇到用户个人或者软件自由保护协会的通知，要求其履行开源协议的义务。虽然目前在国内环境下，开源协议的履行尚未得到司法确认，但是已经有了承认开源协议效力的判例。企业应当尽早了解风险，做好风险预防，在面临相关风险前培养自身抵抗风险的能力。

2.技术进出口合规审核

除了开源软件的进出口限制，企业还应当依据购买软件时技术出口方国家的技术进出口措施进行合规审核。在目前复杂多变的国际政治经济形势下，大国之间的博弈也常常体现在技术进出口限制方面。美国曾发布相关措施限制人工智能软件的出口，限制出口的软件包括应用于智能化传感器、无人机、卫星和其他自动化设备的目标识别软件（无论民用或军用）等。企业一旦落入或者违反相关规范，可能导致被制裁的后果，对未来在该国从事商业活动造成严重影响。

3.专利前置审核

由于开源软件的许可证不一定明示了专利许可，因此，在使用他人的开源代码前，应当根据使用地域对当地的专利注册情况进行检索。如果权利人已经在先注册专利，那么该开源代码使用方式就受到了限制，企业应当根据自身需求，判断是否能够继续利用该开源代码以及如何利用。

4.开源方式审核

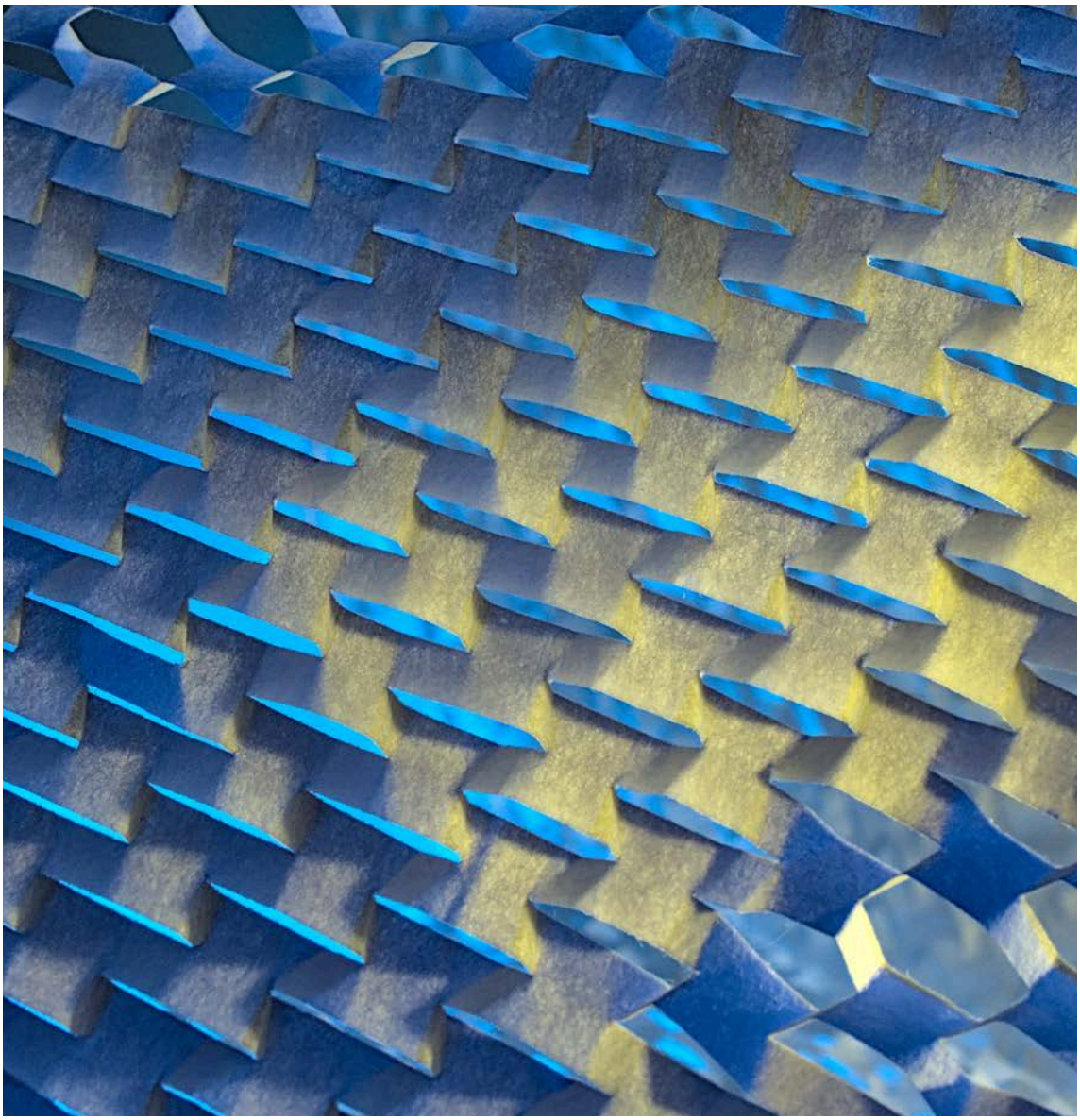
选择合适的许可方式是保证可持续性发展的前提，企业可以以专有许可、开源许可证或者双重许可的方式选择是否对公众发布产品的源代码，以及后续以何种方式更新。如果一项成果是基于已有作品修改完成的，那么它最好符合原作品许可协议的要求，因为协议中有可能要求它遵从相同的许可证发布。对于不值得更新的小程序来说，使用GPL是不适宜的，因为它无法发挥自身传递性的优势，刺激后人对开源的软件进行补充、修改或者更新。

5.软件尽职调查中的开源风险审核

如前所述，人工智能技术离不开开源软件的支持，在并购交易中，如涉及人工智能企业或者其他软件研发企业，对其软件进行开源风险核查是十

分必要的。通过对软件使用的开源软件、开源协议的调查可以识别相应的商业软件本身是否存在开源风险、安全漏洞或者质量问题，使用方是否已经履行了许可协议相关的义务，为交易双方的安全交易提供法律保障。

王红燕
合伙人
知识产权部
杭州办公室
+86 571 5662 3968
gracewang@zhonglun.com



人工智能技术的可专利性探析

作者/张鹏

1.刘鑫、覃楚翔："人工智能时代的专利法：问题、挑战与应对"【J】,载于《电子知识产权》2021年第1期。

2.刘鑫、覃楚翔："人工智能时代的专利法：问题、挑战与应对"【J】,载于《电子知识产权》2021年第1期。

人工智能技术可专利性是人工智能技术专利保护的基础性问题。随着人工智能技术专利申请数量的大幅增加，是否构成专利法保护的客体成为法律实践中的重要争议点。人工智能作为当前最为尖端的科技成果，对于专利制度的挑战是全方面的，既包括人工智能技术本体的专利法律保护、人工智能发明成果的专利法律规制，还涉及人工智能应用工具的专利法律影响问题[1]。这其中，人工智能技术本体的可专利性问题，也就是人工智能技术能否纳入专利法保护客体范围，是上述专利制度面临的首要问题。只有明确哪些人工智能技术能纳入专利法保护客体范围，才能进一步明确这些人工智能技术的新颖性和创造性判定、专利文件撰写要求、权利归属、保护范围、侵权判定、侵权救济等。

世界知识产权组织《技术趋势报告2019——人工智能》显示，随着人工智能创新的快速发展，全球人工智能相关专利申请以平均每年28%的速度增长，尤其是在2012年以后增长非常迅速，人工智能相关专利申请主要集中在机器学习、神经网络等领域，申请量最高的20家公司主要来自日本、美国、中国。我国国家工业信息安全发展研究中心、工业和信息化部电子知识产权中心发布的《2020人工智能中国专利技术分析报告》表明，截至2020年10月，中国人工智能专利申请量累计已达69.4万余件，同比增长56.3%，中国人工智能技术专利申请总量首次超过美国，成为全球申请数量最多的国家。

随着人工智能技术专利申请的迅速增加，迫切需要从法律实务层面明确可专利性的判定标准。由于人工智能技术以算法模型作为核心创新点，在专利申请的审查复审和授权专利的无效宣告请求审查程序中，通常会在是否构成专利法保护客体【亦即是否满足《中华人民共和国专利法》（以下简称"**《专利法》**"）第2条第1款关于发明的定义，是否属于《专利法》第25条专利保护排除对象中的"智力活动的规则和方法"】产生较大争议，本文对该法律问题进行分析探讨。

PART 01
人工智能技术的本质属性：算法模型+应用场景

人工智能的本质属性在于算法模型与应用场景的结合，核心是算法创新。通常而言，人工智能技术是以技术算法为基础、在"大数据"与"大计算"的共同驱动下融入多技术领域、不同功能维度的多项单一技术方案所形成的综合性技术束[2]。人工智能是人类社会的伟大发明，同时也存在着巨大的社

会风险[3]。专利制度对人工智能技术创新的回应，需要从人工智能的技术本质出发，既要考虑激励创新创造也要考虑社会风险控制。人工智能技术通常包括基础层、感知层、认知层、应用层四个层次，基础层是实现大计算驱动和大数据保障的基础算法，感知层主要体现为语音技术、图像技术、视频技术、AR/VR增强现实基础等感知性技术，认知层主要体现为人工智能涉及的自然语言处理、知识图谱、用户画像等以机器学习为核心的认知性技术，应用层主要是无人驾驶、智能硬件等应用场景。从技术创新和社会风险控制的角度而言，基础层的基础算法是最为核心的创新，逐层拓展到应用场景的实现。

人工智能技术可专利性面临的本质难题是，基础算法属于智力活动的规则和方法。如前所述，人工智能技术的核心在于基础层的基础算法，然而传统的专利法律制度认为算法属于智力活动的规则和方法，从而人工智能技术理应被排除在专利法的保护范围之外[4]。同时，由于思想表达二分法下仅仅保护作品的表达，使得软件著作权对人工智能基础算法的保护非常有限。此外，技术秘密保护以及反不正当竞争法的行为规制，对人工智能基础算法的保护亦有不足。可见，**人工智能技术可专利性需要考虑如何对基础算法的保护需求加以回应，以及如何在感知层、认知层、应用层的技术方案中实现对基础算法的实质保护。**

3.吴汉东："人工智能时代的制度安排与法律规制"【J】，载于《法律科学》2017年第5期。

4.张洋："论人工智能发明可专利性的法律标准"【J】，载于《法商研究》2020年第6期。

PART 02
人工智能技术的可专利性判断：拟制现有技术排除测试法和技术属性测试法

主要知识产权强国纷纷出台人工智能技术可专利性审查规则。在人工智能技术专利申请数量快速增长的背景下，主要知识产权强国纷纷调整专利审查标准，给出人工智能技术可专利性的判定规则。例如，2018年欧盟发布《欧盟人工智能》战略，推动欧盟在国际人工智能竞争中的地位提升，在该《欧盟人工智能》战略的指导下，欧洲专利局在2018年11月修改了《专利审查指南》，在第G-II-3.3.1节增加了有关人工智能领域创新技术方案的专利审查思路和专利审查方法，从"发明主题"和"技术贡献"两个维度考量可专利性问题；2017年日本振兴战略与人工智能技术战略委员会制定《人工智能技术战略》，在该战略指导下，特别是针对2016年以后日本人工智能、机器学习领域的专利申请成倍增加的情况，日本特许厅在2018年3月出台《面向人工智能相关技术的审查指南实例》，结合具体案例给出了人工智能基础算法、

人工智能基础算法与应用场景相结合的方案的可专利性审查标准；美国早在2011年就出台了《国家机器人计划》，2017年进一步出台《国家机器人计划2.0》和《人工智能未来法案》，2019年进一步签署《人工智能倡议行政命令》，在上述公共政策指导下，美国专利商标局于2019年1月发布《专利保护客体审查指南（2019年修改版）》（*The 2019 Revised Patent Subject Matter Eligibility Guidance*）[5]，这一审查规则也适用于人工智能算法相关的专利申请的审查。

1.美国针对人工智能技术可专利性判定的法律实践进展：拟制现有技术排除测试法[6]

美国针对人工智能技术可专利性判定采取拟制现有技术排除测试法，将涉及抽象概念的部分拟制为对专利新颖性和创造性不具有任何贡献的现有技术，在新颖性和创造性判断中加以排除。《美国专利法》第101条规定，凡发明或者发现任何新颖而实用的方法、机器、产品、物质合成，或者其任何新颖而实用之改进者，可按照本法所规定的条件和要求获得专利。对于这四类可以受到专利法保护的客体：方法、机器、产品、物质合成，判例法分别给出了定义。亦即，方法，是指处理某些物质使之产生某种特定结果的方式，它是某种行为或者系列行为，作用于客体物质上，使之改变并产生不同的状态或者物[7]；机器，是指整体的机器，整体机器中的一个或者几个部件，一个或者几个部件的合并，以及将原有部件合并起来形成一部机器[8]；物质合成，是指“两种或者更多物质合成的所有物品，以及……所有的合成物品，不论它们是化学合成的结果还是机械性物理合成的结果，不论它们是气体、液体、粉末还是固体[9、10]”。同时，通过司法实践，美国最高法院明确了不授予专利权的客体包括自然规律、物理现象和抽象概念[11]。美国最高法院2014年Alice案形成了“拟制现有技术排除测试法”的基本逻辑，将上述自然规律、物理现象、抽象概念拟制为对专利新颖性和创造性不具有任何贡献的现有技术，在新颖性和创造性判断中加以排除，要求权利要求的其他部分具备新颖性和创造性[12]。对于人工智能技术发明专利而言，尤其需要判断是否属于“抽象概念（abstract idea）”，亦即如何区分受到专利法保护的包含算法特征或商业规则和方法特征的发明专利和属于抽象概念的不属于专利法保护的创新创造。这是由于算法本身更类似于数理逻辑，而与解决技术问题的技术手段存在一定差异。但是，有学者认为，专利法区分抽象思想与具体技术的传统标准并不像诸多学者所想象的那样否定计算机程序算法的客体属性。程序算法是运行独立于人脑的物理系统(计算机)的具体方法步骤,并非抽象的思维

5.参见https://www.federalregister.gov/documents/2019/01/07/2018-28282/2019-revised-patent-subject-matter-eligibility-guidance（2021年7月16日最后访问）。

6.部分内容参见张鹏：“专利审查指南新修改解析：信息通信产业专利授权确权规则新进展”【J】，载于《专利代理》2020年第2期。

7. Cochrane v. Deener, 94 U.S. 780 (1877).

8.Union Sugar Refinery v. Matthesson, 24 F.Case 686(C.C. Mass,1865).

9.Diamond v. Chakrabarty, 444 U.S. 303, 206 U.S.P.Q. 193.

10.李明德：《美国知识产权法（第二版）》【M】，北京：法律出版社2014年4月版，第37页。

11.Diamond v. Chakrabarty, 444 U.S. 303, 206 U.S.P.Q. 193.

12.狄晓斐：“人工智能算法可专利性探析——从知识生产角度区分抽象概念与具体应用”【J】，载于《知识产权》2020年第6期。

规则。程序算法被执行后会导致传统专利法意义上的“物质状态改变”。因此，程序算法符合前述传统标准，可顺利通过客体审查。[13]美国的法律实践也恰恰验证了上述观点。

判断包括人工智能技术在内的、涉及算法的专利申请是否具备可专利性的“三步法”：第一步，是否属于专利法保护客体的法定类别（方法、机器、产品、物质合成）；第二步，是否存在“抽象概念”，如果不存在“抽象概念”，那么属于专利法保护客体，如果存在“抽象概念”，那么除去权利要求“抽象概念”以外的其他部分是否将“抽象概念”转化为了“实际应用”，如果除去权利要求“抽象概念”以外的其他部分将抽象概念转化为了“实际应用”，那么属于专利法的保护客体；第三步，权利要求中除去没有转化为“实际应用”的“抽象概念”的其他部分，是否使得权利要求具备新颖性和创造性，如果是则属于专利法的保护客体，如果否则不属于专利法的保护客体。

美国最高法院Alice案确立针对专利保护客体的两步骤判断方法：首先判断是否属于法定类别（方法、机器、产品、物质合成），其次判断是否属于法定例外（自然规律、物理现象、抽象概念）以及权利要求中是否包含其他特征使得权利要求符合“明显超出”（significantly more than）法定例外的司法例外情形。例如，在Berkeimer v. HP 案中，涉及的数字资产管理系统通过防止相同内容的文字和图片的重复存储的方式，提高效率降低重复率，使得可以通过一次操作改变包含相同存储对象的所有元素。地区法院认为，其不属于专利法保护的客体，因为权利要求中所保护的是仅仅使用公知的、例行的和通常的计算机功能实现的方法步骤。联邦巡回上诉法院则认为，请求保护的方案相对于现有技术提升了效率和计算机功能，针对这样的权利要求采用即决判决（summary judgment）的方式不妥当。美国专利商标局2019年1月7日发布的《专利保护客体审查指南（2019年修改版）》在坚持上述美国最高法院Alice案两步骤判断方法的基础上，对第二步骤进行了修改，在判断是否属于法定例外中的“抽象概念”时，需要判断是否具有实际应用（practical application）。也就是说，如果权利要求将抽象概念整合在一个实际应用中，则符合专利法保护客体的要求；如果权利要求没有将抽象概念整合在一个实际应用中，则需要判断权利要求中是否包含其他特征使得权利要求符合“明显超出”法定例外。对于“具有实际应用”，说服审查员认可符合专利保护客体规定的最简便的方法是，主张该权利要求是计算机功能的提高或者对其他技术的提高。

《专利保护客体审查指南（2019年修改版）》实施以来最为重要的适用案例是，美国专利商标局专利审判和上诉委员会针对Ex parte Eileen C. Smith

13.崔国斌：“专利法上的抽象思想与具体技术——计算机程序算法的客体属性分析”[J]，载于《清华大学学报（哲学社会科学版）》2005年第3期。

案做出的决定[14]。该案件涉及一种在混合交换系统中进行衍生品交易的方法，其权利要求1为，“一种在混合交换系统中交易衍生产品的方法，所述方法包括：通过通信网络和订单路由系统收集订单，并将其放置在电子书数据库中；在电子交易引擎处识别来自第一拥挤市场参与者的新报价，其中新报价中的出价或要约价格中的一个与电子书数据库中来自公共客户的订单中的相应价格相匹配；从电子书数据库中删除至少一部分订单，延迟自动执行新报价和订单，并启动计时器；经由通信网络和电子报告系统，报告指示至少部分订单的执行的市场报价，同时延迟自动执行；在电子交易引擎处接收到来自第一人群市场参与者的新报价之后，在计时器到期之前，从第二人群市场参与者处接收第二报价，其中第二报价与公共客户的相应价格匹配在电子书数据库中订购；在电子交易引擎中的第一和第二拥挤市场参与者之间分配订单，其中直到计时器到期才执行该订单。”美国专利商标局专利实质审查部门认为，该专利申请属于抽象概念，不属于专利法的保护客体。专利审判和上诉委员会撤消了上述驳回决定。其认为，根据《专利保护客体审查指引（2019修改版）》，权利要求1的特征列举了衍生产品交易环境中发生的一些操作，在判断是否属于法定例外中的“抽象概念”时，需要判断是否具有实际应用。权利要求1列举了各种与计算机实现相关的限定，例如“混合交换系统”、“通信网络和订单路由系统”、“电子交易引擎”、“电子书数据库”和“电子报告系统”。尽管这些与计算机实现相关的限定是与电子衍生产品交易特定的限定，但是说明书中并没有特别限定其结构或者配置，因此，这些与计算机相关的限定不足以构成实际应用的司法例外。同时，专利审判和上诉委员会指出，权利要求1具有解决在电子环境和交易大厅同时进行的混合交易系统所产生的问题，这些限定包括：（1）“延迟自动执行新报价和订单，并启动计时器”；（2）在“延迟自动执行”订单后并且在“计时器到期之前”，接收第二报价，“其中第二报价与公共客户的相应价格匹配在电子书数据库中订购”；（3）“在电子交易引擎中的第一和第二拥挤市场参与者之间分配订单，其中直到计时器到期才执行该订单”。这些限定使得权利要求将抽象概念整合在一个实际应用中，从而符合专利法保护客体的规定。据此，专利审判和上诉委员会撤消了驳回决定。

2.欧盟针对人工智能技术可专利性判定的法律实践进展：技术属性测试法[15]

欧盟坚持以“技术性”作为专利保护客体的判定标准，重点考察人工智能技术是否具备技术属性。《欧洲专利公约》第52条规定了“可以取得专利的

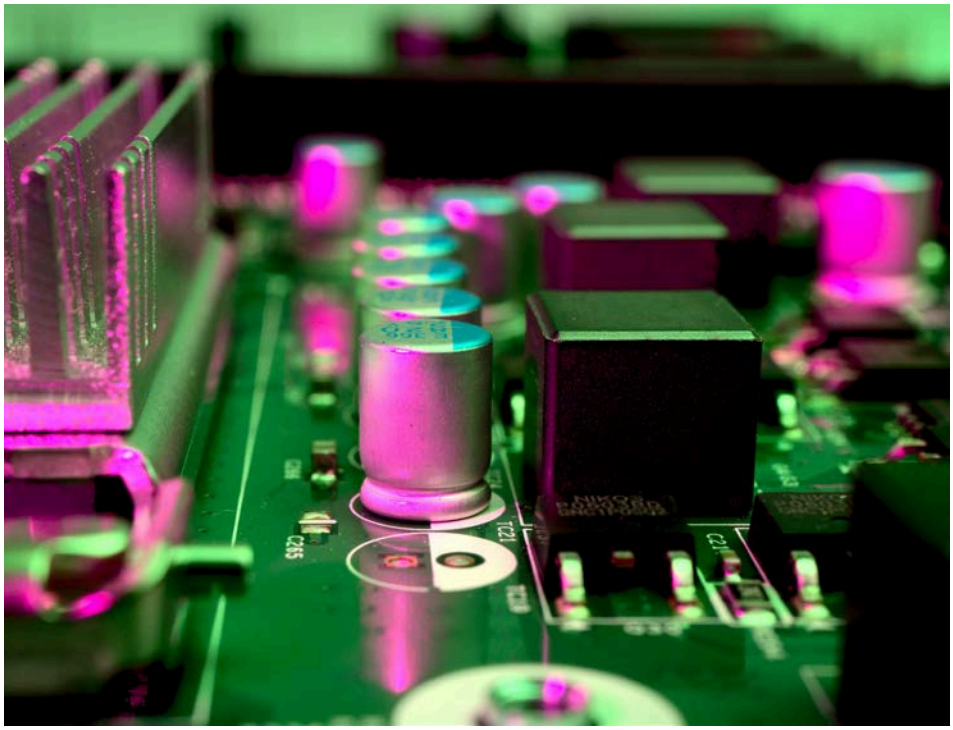
14.参见Ex parte Eileen C. Smith, Appeal 2018-000064, Application 13/715,476.

15.部分内容参见张鹏：“专利审查指南新修改解析：信息通信产业专利授权确权规则新进展”【J】，载于《专利代理》2020年第2期。

发明”：其中第1款规定，“对于任何有创造性并且能在工业中应用的新发明，授予欧洲专利。”第2款规定，“下列各项尤其不应认为是第一款所称的发明：a）发现科学理论和数学方法；b）美学创作；c）执行智力行为、进行比赛游戏或经营业务的计划、规则和方法，以及计算机程序；d）情报的提供。”第3款规定，“第二款的规定只有在欧洲专利申请或欧洲专利涉及该项规定所述的主题或活动的限度内，才排除上述主题或活动取得专利的条件。”可见，欧洲专利法律规则将计算机程序和智力活动的规则方法排除在专利法保护的客体范围内。欧洲专利局《专利审查指南》对此进一步细化，其中指出《欧洲专利公约》第52条第1款规定的“发明”必须是具体的技术方案，第二款对排除在专利法保护客体之外的主题作出了非穷举性列举。在进行客体判断时，需要将权利要求保护的整体方案视为一个整体判断是否具有技术特征，这一判断是在不考虑现有技术状况的前提下进行的。只要具有技术特征，就需要评估每一个特征（包括技术特征和非技术特征）在发明中是否对要求保护的主题作出了贡献。

欧洲专利局2018年11月修改的《专利审查指南》将人工智能作为数学方法的例外，强调数学方法本身不具备技术属性，数学方法的技术应用和技术实施具备技术属性。2018年11月，欧洲专利局在《专利审查指南》Part G Chapter II 第3.3.1节增加了有关人工智能领域创新技术方案的专利审查思路和专利审查方法，从“发明主题”和“技术贡献”两个维度考量可专利性问题。原《专利审查指南》G部分“专利性”第 II 章“发明”第3节“排除的主题”明确排除在专利法保护的客体范围之外的主题包括：发现，科学理论，数学方法，美学创作，智力活动、游戏或者商业方案、规则和方法，计算机程序，信息呈现（主要包括用户界面和数据获取、格式和结构）。其中，在“数学方法”部分增加了“技术应用”、“技术实施”，大幅调整“智力活动、游戏或者商业方案、规则和方法”的审查规则，在“计算机程序”部分增加了“计算机实施的发明”，包括信息建模、编程活动和编程语言，数据获取、格式和结构，并且将“数据获取、格式和结构”从原《专利审查指南》的“信息呈现”部分移入2018年新《专利审查指南》的“计算机实施的发明”部分。可见，上述修改都是与ICT产业涉及包含算法特征或商业规则和方法特征的发明专利申请相关。具体解读如下：

第一，在“数学方法”部分增加了“技术应用”和“技术实施”。2018年欧洲专利局《专利审查指南》全面改写了原《专利审查指南》这一部分的内容，首先明确了“数学方法在解决各个技术领域的技术问题起着重要的作用”。并将规则明确为，如果权利要求仅仅涉及抽象的数学方法而不需要任何技术



手段（例如仅仅制定数学方法的数据或者参数的技术性质），则排除在专利法保护客体之外；如果权利要求涉及使用技术手段（例如计算机）的方法或者设备，则该主题整体上具有技术特征从而不应排除在专利法保护客体之外。2018年欧洲专利局《专利审查指南》在“数学方法”部分增加了“技术应用”、“技术实施”。就技术应用而言，评估数学方法对发明作出的贡献时需要考虑该数学方法是否用于特定的技术目的，例如通过测量压实机的经过次数确定所需材料密度，属于用于技术目的的数学方法，而诸如“控制技术系统”的目的（并非特定的技术目的）并不足以赋予数学方法技术应用的特性。就技术实施而言，如果权利要求是针对数学方法的特定技术实施，并且有计算机驱动使得该数学方法特别适用于该实施，则该数学方法的技术实施符合保护客体要求。反之，如果数学方法并不用于技术目的并且技术实施并未超出一般实施的范围达到特定技术实施的程度，则不属于保护客体。

进而，2018年《专利审查指南》在该部分进一步针对人工智能和机器学习，模拟、设计或者建模，作出具体规则。一方面，人工智能和机器学习。人工智能和机器学习领域的发明专利申请，需要区分基于分类、聚类、回归和降维的计算模型和算法，与计算模型和算法在各种技术领域的具体应用。神经网络、遗传算法、支持向量机、K均值、核回归等分类、聚类、回归和降维的计

算模型和算法，本身具有抽象的数学性质，神经网络、推理引擎、支持向量机这样的表述，通常属于缺乏技术性的抽象模型。与之对比，如果分类方法应用于技术目的，生成训练集的步骤和训练分类器支持技术目的的实现，则应当认为作出了技术贡献。另一方面，模拟、设计或者建模。模拟、设计或者建模的权利要求通常属于数学方法或者智力活动。在计算机辅助设计特定产品、系统或者过程的情况下，需要判断所确定的与技术对象的功能有内在联系的技术参数是否基于技术考虑，如果基于技术考虑则具有技术目的。

第二，大幅调整“智力活动、游戏或者商业方案、规则和方法”。原《专利审查指南》对此部分作出统一的笼统规定，2018年《专利审查指南》对“智力活动的方案、规则和方法”，“游戏的方案、规则和方法”和“商业活动的方案、规则和方法”作出区分，并分别加以规定。首先，如果一项方法权利要求中的所有方法步骤都是由智力活动实现的，则属于不受专利法保护的智力活动的方案、规则和方法；如果要求保护的方法需要使用技术手段（例如计算机、测量装置等）来执行其中至少一个步骤，或者如果其将物理实体作为产物，那么不是智力活动的方案、规则和方法。其次，如果权利要求保护的主题限定了实施游戏规则的技术手段，那么其具备专利法所规定的技术特性，同时游戏规则本身或者游戏规则本身的纯自动化实现不能给权利要求带来创造性，需要从工程师或者游戏程序员的角度来评估游戏规则实现的创造性，该技术人员的任务是实现由游戏设计者给予他的游戏规则。还有，如果权利要求保护的主题限定了商业方法至少一些步骤是通过技术手段实现的，例如计算机、计算机网络、可编程装置等，那么其仍然属于专利法的保护客体，需要根据哪些特征对发明技术特性作出了贡献来判断其新颖性和创造性。

第三，在“计算机程序”部分增加了“计算机实施的发明”。计算机程序本身被排除在专利法保护客体的范围之外，但是该排除并不适用于具有技术特性的计算机程序。也就是说，如果计算机程序在计算机上运行时产生了“进一步的技术效果”，则可以成为受到专利法保护的客体。其中，“进一步的技术效果”，是指超出计算机程序与运行计算机程序的计算机硬件之间的正常的物理交互的技术效果。例如，计算机中的电流循环，其本身不足以赋予计算机程序技术特性；控制技术过程或者计算机本身的内部功能或者界面，可以赋予计算机程序技术特性；指定控制汽车的防抱死制动系统、压缩视频、恢复失真的数字图像等，均属于产生了进一步的技术效果。另外，将“涉及计算机、计算机网络或者其他可编程装置的权利要求表达，其中至少一个特征是由计算机程序实现的”称为“计算机实施的发明”，如果采用计算机实施方法、计算机可读存储介质或者设备的权利要求的方式则由于使用了相

应的技术手段而具备技术特性。

进一步，“计算机实施的发明”部分规定了“信息建模、编程活动和编程语言”。通常而言，信息建模是系统分析人员在软件开发第一阶段进行的对现实世界系统或者过程的描述，是缺乏技术特性的治理活动，从而信息建模的建模语言规范、信息建模过程结构、信息模型固有属性、信息模型维护均没有技术特性。如果发明的上下文描述了用信息模型解决特定技术问题，那么可以赋予其技术特性。编程活动是一种非技术性智力活动，只要不是在具体应用或者环境中使用并且产生技术效果，那么就不属于专利法保护客体。例如，面向对象编程，虽然其有助于程序员更加高效地编写程序，但是其本身没有解决技术问题，不具备技术特性。

3.日本针对人工智能技术可专利性判定的法律实践进展：技术属性测试法基础上的宽松适用

日本在专利法保护客体判定方面采用与欧盟类似的“技术属性测试法”，要求其构成技术方案才能获得专利法保护，同时针对人工智能技术采用非常宽松的适用标准。人工智能基础算法与应用场景相结合的方案通常认为属于可以受到专利法保护的“技术方案”。如前所述，日本特许厅在2018年3月出台《面向人工智能相关技术的审查指南实例》，结合具体案例给出了人工智能基础算法与应用场景相结合的方案的可专利性审查标准。其中，对于人工智能算法与应用场景相结合的发明创造，明确属于专利权的保护客体。《面向人工智能相关技术的审查指南实例》给出的一个示例是“一种基于宿舍声誉的文本数据促使计算机设备用于输出合格的宿舍声誉值的训练模型”，其利用神经网络处理文本信息，对文本数据中反应宿舍声誉的特别词汇出现的频率进行分析，提取关于宿舍情况的字段，综合分析所有字段运用训练模型得到一个合理的宿舍声誉评价值。《面向人工智能相关技术的审查指南实例》认为，上述方案利用硬件资源实现了软件的信息处理，属于可以受到专利法保护的“技术方案”。

PART 03
我国人工智能技术可专利性判断实务：两大测试法并用

我国2019年底的《专利审查指南》修改主要针对包括人工智能技术在内的算法特征+应用场景的发明专利申请。与上述知识产权强国相对应的是，我国也于2019年12月31日发布《关于修改<专利审查指南>的公告（第343

号公告）》，对“包括算法特征或者商业规则和方法特征的发明专利申请”的审查基准进一步调整，虽然并非专门针对人工智能技术，但是基于人工智能技术的核心在于算法，从而对人工智能技术相关专利申请的审查有较高的指导意义。此次修改内容已经于2020年2月1日开始实施。此次修改的突出特点是，并非像历次修改一样对《专利审查指南》的相关部分举行局部修改调整，而是现行《专利审查指南》第二部分第九章第1-5节之后增加了完整的第6节，专门针对“包含算法特征或商业规则和方法特征的发明专利申请审查”作出相关规定。可见，此次修改专门针对涉及人工智能、互联网+、大数据以及区块链等的发明专利申请，针对其包含算法或商业规则和方法等智力活动的规则和方法特征的特点，形成专门的审查规则。就《专利审查指南》第二部分第九章此次修改内容与《专利审查指南》第二部分第九章第2-5节的关系而言，构成特别法与一般法的关系。《专利审查指南》第二部分第九章第2节是“涉及计算机程序的发明专利申请的审查基准”，《专利审查指南》第二部分第九章此次修改内容所增加的第6节所针对的“包含算法特征或商业规则和方法特征的发明专利申请”，基本上属于“涉及计算机程序的发明专利申请”。

从《专利审查指南》第二部分第九章此次修改内容给出的9个案例来看，全部属于涉及计算机程序的发明专利申请。因此，《专利审查指南》第二部分第九章此次修改内容，属于《专利审查指南》第二部分第九章第2-5节的特别法，按照同一位阶规范性法律文件特别法优于一般法的规则，针对包含算法特征或商业规则和方法特征的发明专利申请，优先适用《专利审查指南》第二部分第九章此次修改内容。就《专利审查指南》第二部分第九章此次修改内容与涉及人工智能技术的发明专利申请审查规则而言，属于抽象规则与具体适用对象的关系。在审查实践中，判断《专利审查指南》第二部分第九章此次修改内容是否适用，并非需要从发明主题上判断所涉专利申请是否属于涉及人工智能技术的发明专利申请，而是需要从权利要求所要求保护的技术方案的角度判断是否属于“包含算法特征或商业规则和方法特征的发明专利申请”，重点在于审查权利要求所要求保护的技术方案是否包含算法特征或者商业规则和方法特征。如何判断权利要求所要求保护的技术方案是否包含算法特征或者商业规则和方法特征?所谓“算法”，是一系列解决问题的清晰指令构成的用系统方法描述解决问题的策略机制。可见，包含算法特征的核心在于包含用系统方法解决问题的机制，包含解决问题的方法流程。此次《专利审查指南》第二部分第九章的修改，旨在于明确核心创新点在于算法的发明专利申请的客体审查，进一步扩大可以受到专利法保护的、能

够通过客体审查的算法发明创造，以期对核心创新点在于算法的发明创造给予全面的知识产权保护。

我国人工智能技术是否属于专利法保护客体的审查标准，近似于欧盟“技术属性测试法”和美国“拟制现有技术排除测试法”二者取交集，亦即需要满足两个方面的要求才能属于我国专利法的保护客体。根据修改后的《专利审查指南》的规定，对于人工智能技术这类包含算法特征或商业规则和方法特征的发明专利申请，需要从三个方面进行审查，同时这三个方面具有逻辑联系：首先，审查涉案专利申请是否属于专利法意义上的保护客体；其次，审查权利要求是否以说明书为依据，清楚、简要地限定要求专利保护的范围；最后，审查权利要求是否具有新颖性和创造性。亦即，首先，审查涉案专利申请是否属于专利法意义上的保护客体（亦即根据《专利法》第25条第1款第（二）项和《专利法》第2条的审查），这一点类似于欧盟“技术属性测试法”；其次，审查权利要求是否以说明书为依据，清楚、简要地限定要求专利保护的范围；最后，审查权利要求是否具有新颖性和创造性，这一点类似于美国“拟制现有技术排除测试法”。此次《专利审查指南》修改强调的是，在上述三个方面的判断上，注重从整体角度考虑“技术特征以及与技术特征功能上彼此相互支持、存在相互作用关系的算法特征或商业规则和方法特征”，从而使得第一个条件（符合保护客体要求）降低，同时提高第二、三个条件，平衡地保护专利申请人和社会公众的利益。

首先，在审查人工智能专利申请是否属于“技术方案”时注重整体性。《专利审查指南》修改稿强调，“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。” 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，需要整体考虑权利要求中记载的全部特征。可见，在这一过程中，技术特征与算法特征或商业规则和方法特征之间的关联程度或者关系紧密程度，是判断的关键。下面以国家知识产权局之前的审查实践作为验证：

在第10713号复审请求审查决定中，国家知识产权局认定，“权利要求1请求保护一种用于提高经过计算机系统互联网来订购产品的安全性的方法。该解决方案是利用公知的计算机和网络技术进行产品订购，在计算机和服务器之间通过互联网建立网络连接进行网上交易，其中使用直接连接来传送密钥以保证交易的安全性。该解决方案虽然结合了直接连接作为安全通道或者安全链路来传送密钥，但使用直接连接作为安全通道或者安全链

路来传送密钥是本领域公知的技术，将用户的订购信息和其自身的身份信息（如标识、密钥等）分别在不同的通道传输，既没有给该网络的数据传输、内部资源管理等内部性能带来改进，也没有给现有计算机系统和服务器的构成或功能带来任何技术上的改变。该方案的目的在于如何顺利进行网络交易，并不在于脱离网络交易而对网络系统本身安全性的改进。该方案所要解决的问题是如何进行网上交易，不构成技术问题，采用的手段只是根据人为制订的规则来实施产品订购的方法，不是技术手段，获得的效果只是对交易过程的管理和控制，也不是技术效果，所以权利要求1不属于专利保护的客体。”

与之对比，在10720号复审请求审查决定中，国家知识产权局认为，“权利要求1要求保护一种信息通知方法，该方案针对背景技术存在的在报表明细传输过程中无法避免使用人力，即传递人员必需通过计算机输入对方的邮件地址或在传真机上输入号码，因此费时费力、没有效率的问题，权利要求1的方法所要解决的问题是通过网络系统将报表明细完成编辑后自动将通知信息传送至需要接收的单位的信息接收装置，因此属于信息传输中的技术问题；并且为了完成自动传送包括报表的通知信息，该方法采用了建立接收单位基本数据库，信息通知系统判断是否接收到一通知信息，读取该通知信息并取出接收单位的相关资料，根据接收单位的相关资料找出与其对应的联络资料，信息通知系统将通知信息传送至信息接收装置等手段，通过对网络系统、信息接受装置、信息通知系统等进行控制，实现了将通知信息自动传送至接收装置，因此是利用了遵循自然规律的技术手段；获得的是使用计算机网络自动传送信息并提高信息通知处理效率，从而节省人力、时间的技术效果。由于该方法所解决的问题、采用的手段和获得的效果都具有技术性，所以权利要求1属于专利保护的客体。”从审查实践来看，上述将权利要求保护的整体方案视为一个整体判断是否具有技术特性的基本思路，亦即对于是否具有技术特性的判断是在不考虑现有技术状况的前提下进行的基本做法[16]，与欧洲专利局“技术属性测试法”基本一致。

其次，在审查涉案专利申请的权利要求是否得到说明书支持以及是否清楚时注重整体性。《专利审查指南》修改稿强调，“包含算法特征或商业规则和方法特征的发明专利申请的权利要求应当以说明书为依据，清楚、简要地限定要求专利保护的范围。权利要求应当记载技术特征以及与技术特征功能上彼此相互支持、存在相互作用关系的算法特征或商业规则和方法特征。”可见，在判断是否得到说明书支持以及权利要求是否清楚时应当考虑技术特征与算法特征或商业规则和方法特征之间的内在逻辑联系。

16.《专利审查指南》规定，“如果权利要求涉及抽象的算法或者单纯的商业规则和方法，且不包含任何技术特征，则这项权利要求属于专利法第二十五条第一款第（二）项规定的智力活动的规则和方法，不应当被授予专利权。……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。”通常而言，专利法第二十五条和第二条的审查也是在未对现有技术进行检索过程前进行的。

还有，在审查涉案专利申请的权利要求是否具备新颖性和创造性时注重整体性。对既包含技术特征又包含算法特征或商业规则和方法特征的发明专利申请进行创造性审查时，应将与技术特征功能上彼此相互支持、存在相互作用关系的算法特征或商业规则和方法特征与所述技术特征作为一个整体考虑。“功能上彼此相互支持、存在相互作用关系”是指算法特征或商业规则和方法特征与技术特征紧密结合、共同构成了解决某一技术问题的技术手段，并且能够获得相应的技术效果。可见，修改后的《专利审查指南》对人工智能技术专利申请的新颖性和创造性审查，建立了两个规则：全面考虑规则和整体考虑规则。其中，“全面考虑规则”是指，对包含算法特征或商业规则和方法特征的发明专利申请进行新颖性审查时，应当考虑权利要求记载的全部特征，所述全部特征既包括技术特征，也包括算法特征或商业规则和方法特征。“整体考虑规则”是指，对既包含技术特征又包含算法特征或商业规则和方法特征的发明专利申请进行创造性审查时，应将与技术特征功能上彼此相互支持、存在相互作用关系的算法特征或商业规则和方法特征与所述技术特征作为一个整体考虑。“功能上彼此相互支持、存在相互作用关系”是指算法特征或商业规则和方法特征与技术特征紧密结合、共同构成了解决某一技术问题的技术手段，并且能够获得相应的技术效果。对于新颖性创造性判断的非技术特征考量这一点，我国修改后的《专利审查指南》与欧洲2018年《专利审查指南》秉持的贡献论存在较大差异，使得专利申请更容易通过新颖性创造性的审查。同时，正如上文所引述的Ex parte Eileen C. Smith案审查决定，在认定“‘延迟自动执行新报价和订单，并启动计时器’等特征使得权利要求将抽象概念整合在一个实际应用中，从而符合专利法保护客体的规定”时，将功能上彼此相互支持、存在相互作用关系的技术特征与算法特征进行了整体考虑，美国这一思路与我国是一致的。

由于我国对于人工智能技术这类包含算法特征或商业规则和方法特征的发明专利申请需要从三个方面进行审查，既要满足类似“拟制现有技术排除测试法”的要求，也要满足类似“技术属性测试法”的要求，由此导致我国人工智能技术专利申请的授权确权存在相当的难度。

PART 04
人工智能技术专利授权确权实务建议：专利布局+撰写规范

如前所述，我国要求人工智能技术既要满足类似“拟制现有技术排除测试法”的要求，也要满足类似“技术属性测试法”的要求才能获得授权，由此

使得人工智能技术专利授权确权存在相当的难度。这一方面需要我们积极呼吁完善《专利审查指南》中的相关规则，进一步拓展人工智能技术的可专利性范围，特别是针对一定范围的基础算法创新纳入专利法的保护客体范围；另一方面，也需要我国人工智能企业立足现有审查规则开展人工智能技术的专利授权确权实务工作。具体如下：

一是加强人工智能技术专利布局。如前所述，我国国家工业信息安全发展研究中心、工业和信息化部电子知识产权中心发布的《2020人工智能中国专利技术分析报告》表明，截至2020年10月，中国人工智能专利申请量累计已达69.4万余件，同比增长56.3%，中国人工智能技术专利申请总量首次超过美国，成为全球申请数量最多的国家。由此可见，我国人工智能技术的专利申请快速增长，专利布局的空白点在日益减少。即使我国人工智能技术审查规则存在一些障碍，我们仍然需要积极开展人工智能技术的专利布局，运用多种专利类型开展人工智能技术的专利保护。

二是加强人工智能专利文件的撰写规范。由于我国要求人工智能技术既要满足类似“拟制现有技术排除测试法”的要求，也要满足类似“技术属性测试法”的要求才能获得授权，我们需要通过专利文件的撰写技巧，充分利用权利要求的解释规则，加强人工智能专利文件的撰写规范。特别是人工智能创新的核心是基础算法，基础算法需要在特定撰写方式下才能够获得专利权保护。特别需要注意的是，由于思想表达二分法下仅仅保护作品的表达，使得软件著作权对人工智能基础算法的保护非常有限；技术秘密保护以及反不正当竞争法的行为规制，对人工智能基础算法的保护亦有不足，我们需要通过撰写技巧的安排将人工智能基础算法满足可专利性的要求，积极获得人工智能基础算法的专利保护。

张鹏
合伙人
知识产权部
北京办公室
+86 10 5957 2068
zhangpeng@zhonglun.com

人工智能领域非专利实施主体（NPE）的威胁与应对

作者/顾萍、贾媛媛、王成荫

人工智能技术在近几年取得了突破性的发展，在机器视觉、语音识别、气象预测、大数据分析等方面，人工智能技术在人们生活中的应用越来越广泛，为人们的生产生活、沟通交流带来了更多的便利。人工智能技术主要通过计算机运算来模拟人的思维流程，以完成复杂的任务。当下，人工智能技术正加速地渗透到各行各业的研发、生产活动中，为人们带来了远程医疗、自动驾驶、智能电网等“科幻性”的技术。

新型的技术形态会为知识产权保护带来新的挑战，未来，NPE在人工智能领域的活动极大可能会成为影响相关科技快速发展的因素之一。NPE全称Non-Practicing Entities，即非专利实施主体。NPE一般不会自行研发，而是会选择低价购买小中企业或发明人所拥有的具有市场前景的专利，然后寻找市场上运用类似技术成果的企业，以诉讼威胁或提起诉讼为手段，迫使对方支付许可费；或通过法院判决得到赔偿金而获利。本文梳理了人工智能领域侵权诉讼的难点以及NPE诉讼的特点，就人工智能领域NPE的威胁与应对进行了深入探讨，以供相关人员参考。

PART 01

NPE的特点

1.1 NPE概念及分类

NPE全称Non-Practicing Entities，即非专利实施主体，是一个中性词，NPE可以包括高校、专业研究院所及个人研发者，同时也可以包括从其他公司、研究机构或个体发明人手中购买专利的所有权或使用权、然后专门通过专利诉讼赚取巨额利润的公司或团体。

通常认为，目前在中国活动的NPE大致分为四类，即科研型NPE、转化型NPE、中介型NPE及投机型NPE。其中，投机型NPE即类似于通常所述的“专利流氓”或“专利蟑螂”，也称诉讼型NPE，这类投机型NPE对于整个市场的影响也最大（本文中以下所述NPE均指的是投机型NPE）。

1.2 投机型NPE的特点

投机型NPE低价购买专利，以诉讼为手段威胁市场上成功的公司，勒索许可费或通过法院判决得到赔偿金而获利。这些NPE的行为无端地增加了产品的摊销成本、减少了产品生产商的利润。任凭NPE肆虐无益于激励创新。

NPE倾向于在具有较大市场发展潜力的技术领域布局，尤其喜欢布局模糊的、权利要求不具体的专利。因此，NPE的活动在包括软件领域在内的高新技术领域相对频繁。在这些领域的很多专利中，权利要求通常具有效果性特征或者功能性特征，权利要求保护范围模糊。在诉讼过程中，NPE可以主张对于这些权利要求的多种解释，进而扩大解释这些专利的保护范围。因此即便目标公司提前作了必要的FTO检索和侵权分析，其可能也无法明确地规避这类专利的侵权风险。NPE在利用这些模糊的专利骚扰高科技企业时，往往并不向被告、甚至法院提供具体的特征比对表，甚至不明确产品的被诉功能。被诉企业因此无法准确判断自己的产品是否侵权，不能充分地估计诉讼结果，造成很大的应诉压力。由此产生的高额应诉成本和不确定的裁判结果会迫使很多公司接受不公平的和解或授权协议。

NPE通常瞄准在高新技术领域的企业。这些企业产品销量大、利润率高、种类丰富、资金充足，因此更有可能支付较高的赔偿款或和解金。另外，这些高科技企业通常销售比较复杂的产品，在同一件产品上涉及的专利可能会非常多。鉴于一个产品，无论多复杂，只要涉嫌一项专利侵权，法院也可能裁判禁止该产品的生产和销售。因此NPE诉讼通常会给高科技企业造成较大压力。

NPE在发起诉讼之前，通常也会对某领域做深入调研，对行业和相关企业有深入的了解，对诉讼也具有一定的专业性。同时，NPE通常具有专业的诉讼律师以及成熟的诉讼策略。因此，专心经营的企业也要了解和关注NPE的特点，才能有效的应对NPE。

PART 02

人工智能领域NPE的发展趋势及影响

2.1 人工智能领域专利侵权的主要特点

人工智能（AI）是一种在近年来发展迅速的技术领域，一些分析指出，到2030年，人工智能技术的市场会达到150亿美元。随着平行计算芯片的快速迭代，网络云计算的逐步推广，以机器学习算法为主导的人工智能应用在近些年来层出不穷。随着相关市场的不断升温，同业竞争越来越激烈，开发者和企业也逐渐开始重视在人工智能领域的知识产权保护。例如，在美国近十年内与人工智能相关的专利的授权数量成指数倍增长。我国国家知识产权局也在去年开放了人工智能方面的专利申请。一些国际知名的大型跨国企业，如IBM、谷歌、苹果等，都非常重视与人工智能相关的产品开发和专利布局。

作为一种新兴技术，人工智能会给传统的专利侵权判定带来挑战。开发现代AI产品的过程中所需要的直接人工干预远小于传统的计算机软件。在传统的产品开发过程中，人工智能最多只是起到辅助工具的作用，最终的产品是人的智力成果。在这种情况下，侵权行为的主体和客体的认定都相对直接，侵权行为的体现也是相对直观的。相比之下，涉及人工智能的产品的侵权认定则比较复杂。一般来说，人工智能程序的开发流程是：开发者选定训练的模型、提供训练数据和指引；计算机使用模型进行运算；最终得出一个程序。这期间，预期得到的程序经过了多次迭代，开发者没有，或仅仅在一个非常有限的范围内，直接干预最终程序的编写、编译；并且最终得到的程序也可能是动态的、在使用过程中可以自发的改进、更新的。这期间，无论是训练数据、训练模型、训练工具、训练过程中的某一个最终程序的中间形态、还是最终的程序都有可能涉及侵权。并且，一个人工智能程序往往由不同的主体开发、运营、维护，训练工具的提供方也通常是独立主体。因此，一个人工智能程序可能产生的专利侵权贯穿这个程序整体的生命周期，可能涉及多个和这个程序有关系的主体。

2.2 人工智能领域NPE案件的趋势

由于我国国家知识产权局在去年才开放了人工智能方面的专利申请，因此当前该领域已授权专利积累量还不多；但是可以预见，在短期内该领域的专利积累会有火速增长。人工智能领域具有一些适合NPE的独特特点，因此笔者预计，在未来某一阶段，人工智能领域的NPE案件也会呈现出爆炸式发展。

2.2.1 NPE偏爱权利要求范围相对模糊的专利

人工智能行业的诸多特点使与其相关的专利的权利要求中会涉及到大量“效果特征”或者“功能性限定特征”，导致权利要求保护范围相对模糊。因此NPE公司以这一类权利要求提起诉讼时并不需要进行非常充分的特征比对和技术分析。这些相对模糊的权利要求也使得人工智能领域的高科技企业很难准确判断侵权可能性，因此增大了应诉成本。这些企业为了避免不确定的审判结果，更可能会向NPE妥协，与之进行和解。

2.2.2 人工智能领域大多为大型高科技企业，投入巨大、竞争激烈

人工智能领域门槛很高，多数企业属于大型高科技企业，公司生产规模庞大、投入高且技术复杂，产品所涉及专利数量多且关系密切。往往一旦产品的某个功能模块被认定侵犯某项专利权而被颁发禁令，会严重影响这个企业的整体业务。

另外，人工智能领域是当前各国及各大企业争相占领的技术高地，技术积累及更新也非常快，因此专利布局非常密集。不同企业之间的专利布局难免出现交叉和类似之处，NPE比较容易挑选出部分合适的专利发起诉讼。因此该领域密集的专利布局会给NPE带来可乘之机。

2.2.3人工智能领域专利侵权判定过程较复杂，增大被诉企业的应诉成本

人工智能领域市场准入门槛高、产品研发投入高，所以行业内一般有多家体量很大的跨国企业。同时，人工智能领域通常涉及到多领域技术知识的整合。在涉及多领域的侵权案件中，都会给法院审判以及被告做不侵权抗辩造成较大的负担。例如在通信和软件领域，很多具体功能需要通过复杂的技术实现，并且可能会出现多个技术领域的交叉应用；由于涉及到的技术复杂，被告可能需要引入第三方鉴定机构或者本领域技术专家来对技术进行鉴定或分析。这会进一步增加企业的应诉费用和难度，也增加了被告向NPE妥协的可能性。

2.2.4人工智能领域专利侵权通常涉及多个可诉被告，符合NPE的商业模式

对于NPE来说，仅通过一件侵权诉讼即可威胁到多个公司。这样一来，NPE很有可能通过一件诉讼就与多个公司达成和解并收取许可费。由于人工智能领域专利侵权通常会涉及到多个主体，该特点恰恰与NPE的商业模式不谋而合，即NPE通过有限的投入可能带来更丰厚的收益，即更多的被诉主体的参与。总体而言，人工智能领域的这一行业特点是有助于NPE发起诉讼的。

2.2.5 新专利法的实施可能会增加NPE诉讼

修改后的新《专利法》已经于2021年6月1日起施行。新《专利法》加强了立法层面对于专利权人的保护。例如新《专利法》将专利侵权的法定赔偿上限由原来一百万人民币调整为五百万人民币；新《专利法》还引入了惩罚性赔偿制度，会对专利侵权诉讼产生激励的效果。因此，可以预见未来专利侵权诉讼的数量将会增加。赔偿额度的指数倍增也会吸引更多的NPE中国进行诉讼行动。结合NPE的特点考虑，笔者认为，高新技术领域中的NPE诉讼会快速增长。

PART 03

NPE恶意诉讼对于人工智能领域行业发展的影响

整体而言，如果投机型NPE案件激增，会对人工智能领域行业发展带来不确定性。这种不确定性会影响到该行业正常的知识产权发展和技术积累。

3.1 打压相关人工智能领域企业的积极性

人工智能领域多数企业属于大型高科技企业，公司生产规模庞大、投入高且技术复杂，产品所涉及专利数量多且关系密切。如果一个产品因为有可能侵犯一件专利权而被禁止销售，势必导致这个产品的开发者不能有效的收回研发成本、获取利润。

而人工智能领域作为一片快速发展的沃土，也是当前各国争相占领的技术高地。因此各企业为了生存，为了已有产品的继续销售使用，不得不继续布局和加强专利技术的开发。然而，人工智能领域专利丛生，要想完美地绕开所有的专利技术进行开发可能性较低。而专利许可费或者诉讼赔偿费，即使对于大企业来说也是难以承受的。

3.2 可能会对企业的商誉造成影响

NPE不仅会阻碍开发产品的主体公司的技术创新、增加产品成本，而且其为了获取赔偿而使用的威胁手段也可能会对减损这些公司的商誉。市场上的负面消息会使公司的品牌价值受到损害，这对大型企业的商誉影响尤为重要。当媒体中充斥着关于一个公司或者企业的品牌的大量的负面信息时，消费者可能会对这个公司的产品的价值产生怀疑。

3.3 增加了企业成本、企业负担，削弱企业竞争力

NPE引发的专利诉讼、专利许可等带来诉讼、许可的费用支出直接提高了产品成本。尤其是专利诉讼的周期很长，一件专利诉讼往往需要花费两年以上甚至更长时间，长时间的专利侵权诉讼过程也需要公司花。费大量的人力物力来应对，势必给企业带来巨大负担。为了填补损失，部分企业也可能会采取降低未来的生产能力或将这部分成本借机转嫁给消费者等方式，这些举措会带来产品售价的剧增，并最终会损害到消费者的利益，在极大增加企业负担的同时削弱了其竞争力。而且NPE诉讼的成本难以预计，不便于企业在产品定价中进行合理的摊销。这给企业增加了利润的不确定性，不便于企业规划产品产能和远期投资。

PART 04

企业如何应对NPE

NPE诉讼目前在国内仍处于试水阶段，尤其是在新型的人工智能领域更是为数不多。但是人工智能领域的相关案件很可能在未来几年内快速增加，该领域的相关企业必须做好准备。企业应充分了解和重视应对NPE诉讼的策略，以降低不断迭代的NPE手段即将给中国知识产权市场带来的冲击。

4.1 诉讼前如何应对NPE

4.1.1 提高企业自主创新能力，加强专利储备，提升自身专利实力

企业可以从以下两个方面入手加强专利储备：

（1）内部挖掘。企业要注重研发、提高自主创新能力、突破核心技术并通过申请专利使之能被授权和保护，储备高质量专利。

（2）外部引入。有资金实力的企业可以拓宽专利储备思路，适度通过专利购买、公司收购等方式补充业务短板，扩充自身高质量专利储备。在接收外部知识产权之前要作好专利风险的评估，包括对专利权的归属、专利权的稳定性、是否为标准必要专利等都要做详尽、专业的评估后才能决定是否引

入。

4.1.2 进行FTO检索分析

对企业来说，在技术立项、研发及商业化应用前都应通过FTO检索发现专利壁垒、识别侵权风险。首先，企业应当梳理产品所搭载的技术点，有针对性地检索相关技术点。对经检索确定存在侵权风险的专利，企业可通过后续的规避设计、专利许可或提起专利无效等手段来规避或消除。

对尚未发现侵权风险的技术方案，要尽早申请专利，以覆盖和保护自身的技术和产品，不给NPE造成可乘之机。

FTO检索的核心要义是全面，要扫除产品上搭载的技术盲区，不给NPE留下可乘之机。为保证FTO检索的全面性，企业可以采取以下措施：(1) 尽可能在不同的检索数据库中进行全面检索；(2) 尽可能找多名检索人员背靠背就同一检索案进行检索，尽量降低人为因素对检索全面性的影响；(3) 对于技术方案的技术主题的切分务必要准确，从而尽可能覆盖技术方案的所有技术细节。

4.1.3 对于相关专利状态进行监控

人工智能领域专利申请非常活跃，所以除全面进行FTO检索之外，还需要定期监控与自身业务相关的专利申请。如果发现相关性较高的专利申请，应当密切关注其申请过程，适时提交公众意见以阻止其授权。此外，从业企业一旦发现业内企业破产，或NPE取得、受让了高相关性专利，则要保持相当的警惕。

另外，企业还应当增强海外市场专利风险意识。产品进入国外市场前，应做好专利分析，做到适应并能够熟练运用海外市场中的专利游戏规则。

4.1.4 关注诉讼动态，尤其是NPE诉讼动态

在日常经营活动中，密切关注本领域的比较活跃的NPE的诉讼动向，尤其是对于在企业核心技术领域已经对其他企业提起诉讼的NPE，更应当予以重点关注和监控。通过相关NPE的诉讼和其他公共领域的行为，把握NPE的专利组成、申请动向及其他活动特点，分析预判NPE近期的行动。

4.1.5 加强同行业企业间共享和交流

为了应对NPE，很多大型跨国企业都自发地组成了专利团体。在人工智能这个新兴领域，同行企业之间，为了应对NPE，也应当通力合作，交流和分享应对策略和技巧经验。同行业企业之间可以组建预警平台，及时披露、共享行业NPE的相关信息，有效提高单个企业抵御NPE诉讼的能力。

4.1.6 加强合同管理，严控与供应商之间的协议

对于外购产品，合同中的知识产权条款应单列并明确供应商的知识产

权担保义务。这样一方面可在未来NPE诉讼中失利后转移部分赔偿责任，另一方面可在发生NPE危机时促使供应商与企业共同全力应对NPE。

在NPE起诉后，被诉企业应尽快将诉讼信息及任何损失补偿协议内容告知供应商。企业还应注意避免与供应商发生冲突，尽可能与供应商保持统一战线，共同应对NPE诉讼，这样可以对NPE造成更大的压力。

4.1.7 对无法回避的专利提起无效请求

通常为了降低诉讼成本，很多NPE的专利被判定无效后，其可能会放弃后续的行政诉讼程序，转而利用其他的专利权。因此及时对于上述专利提起无效请求以消除隐患对于企业而言是必要且有用的。

因此，对于在FTO以及日常监控中筛查出的高风险专利，如果无法绕开或者绕开成本太高，则应考虑及时对于上述专利提起无效请求。

此外，根据专利法规定，任何人都可以对已授权的专利提起无效请求。因此企业可以根据实际情况，灵活选择合适的策略。

4.2 诉讼过程中如何应对NPE

4.2.1 积极寻求与NPE谈判许可

收到NPE的诉讼请求后，作为相关企业，最首选的途径依然是在应诉的同时积极与NPE进行谈判，寻求和解。专利侵权诉讼时间跨度长，应诉成本高。因此如果NPE索要的和解金额不过高，企业依然应当将其作为首要选项之一。

即便初步谈判破裂，双方也可以随着案件的进程，在包括涉案专利提起无效请求后、在管辖权异议出具裁定后、在无效口审后以及在侵权案件证据交换后等时间点寻找合适的谈判和解契机。

另外，NPE持有大量标准必要专利。标准必要专利持有人需要作出FRAND承诺，即其需要在公平、合理、无歧视的原则下对第三人授予专利。尽管这种承诺可能是权利人向国际标准化组织做出、并且在中国境外做出的，但是我国已经在多份司法文件中表明了FRAND原则在中国对标准必要专利持有人具有约束力。实践中，公司针对涉及标准必要专利的诉讼，可利用FRAND原则及反垄断法与NPE进行谈判，以争取较低的专利许可费。

4.2.2 积极应诉

如果遭遇诉讼，被告企业应克服消极心态，积极应对。要充分了解产品使用的技术是否落入对方的专利权保护范围之内，对方是否获得明确诉权，是否可以申请涉案专利无效等。

典型的应对手段中，首先应考虑程序应对：

1）及时提起专利无效宣告请求

一旦NPE的专利被认定无效，NPE就会失去诉讼的基础。即使不被无效，也很可能使涉诉专利的权利要求范围缩小，迫使NPE减少赔偿数额或降低和解条件。实践中，NPE诉讼中的专利权利要求中通常具有功能性或效果性描述，导致权利要求保护范围相对较大，因此被无效的可能性也较高，因此，在第一时间提起针对涉案专利的无效请求应当是必选应对方案。

2）合理利用管辖等手段

在法律允许的情况下，涉诉企业可以考虑提起管辖权异议，并尝试将案件移送到北京、上海等知识产权审判经验丰富的法院进行审理。NPE一般希望速战速决，例如，为了尽快获得侵权赔偿，NPE通常会选择实体上倾向专利权人、程序上结案速度快的管辖法院。因此被诉方一个有效的应对手段是延缓诉讼进程，例如可以合理利用管辖等手段，以拖待变，增大NPE诉讼成本。

3）实体抗辩

被告方可以在实体上进行以下抗辩：不侵权抗辩、现有技术抗辩、合法来源抗辩等。对于涉及到核心产品、以及技术比较复杂的部分案件，被告方也可以尝试考虑进行鉴定或者引入专家辅助人。

4.2.3 严格适用禁令的抗辩

在目前司法实践中，如果法院认为被告的侵权成立，通常法院会判决被告立即停止侵权行为。但是，对于NPE案件，是否也应当同样采取停止侵权的措施呢？

被告可以尝试从以下方面进行抗辩：NPE并不从事实际投资生产，因此侵犯其专利权并不必然会导致其遭受难以弥补的损害，往往通过损害赔偿便足以使之得到救济，随意地做出停止侵害的判决，不仅会造成惩罚过度的后果，还会有损社会公共利益。所以法院在适用停止侵害责任时，不能仅仅以行为人实施了侵犯知识产权的行为并且该侵权行为仍在继续为由当然地做出停止侵害的判决，而应当综合考虑各方面因素，谨慎地适用停止侵权的罚则。

4.2.4质疑NPE诉讼属于滥用权利，寻求反诉费用

2021年6月3日，最高人民法院发布《最高人民法院关于知识产权侵权诉讼中被告以原告滥用权利为由请求赔偿合理开支问题的批复》（以下简称**《批复》**），即日起实施。

该《批复》指出："在知识产权侵权诉讼中，被告提交证据证明原告的起诉构成法律规定的滥用权利损害其合法权益，依法请求原告赔偿其因该诉讼所支付的合理的律师费、交通费、食宿费等开支的，人民法院依法予以支持。

被告也可以另行起诉请求原告赔偿上述合理开支。”

该《批复》明确和简化了被告以原告滥用权利为由请求赔偿合理开支问题的救济范围及救济方式，必将对于知识产权的侵权诉讼产生重大影响。

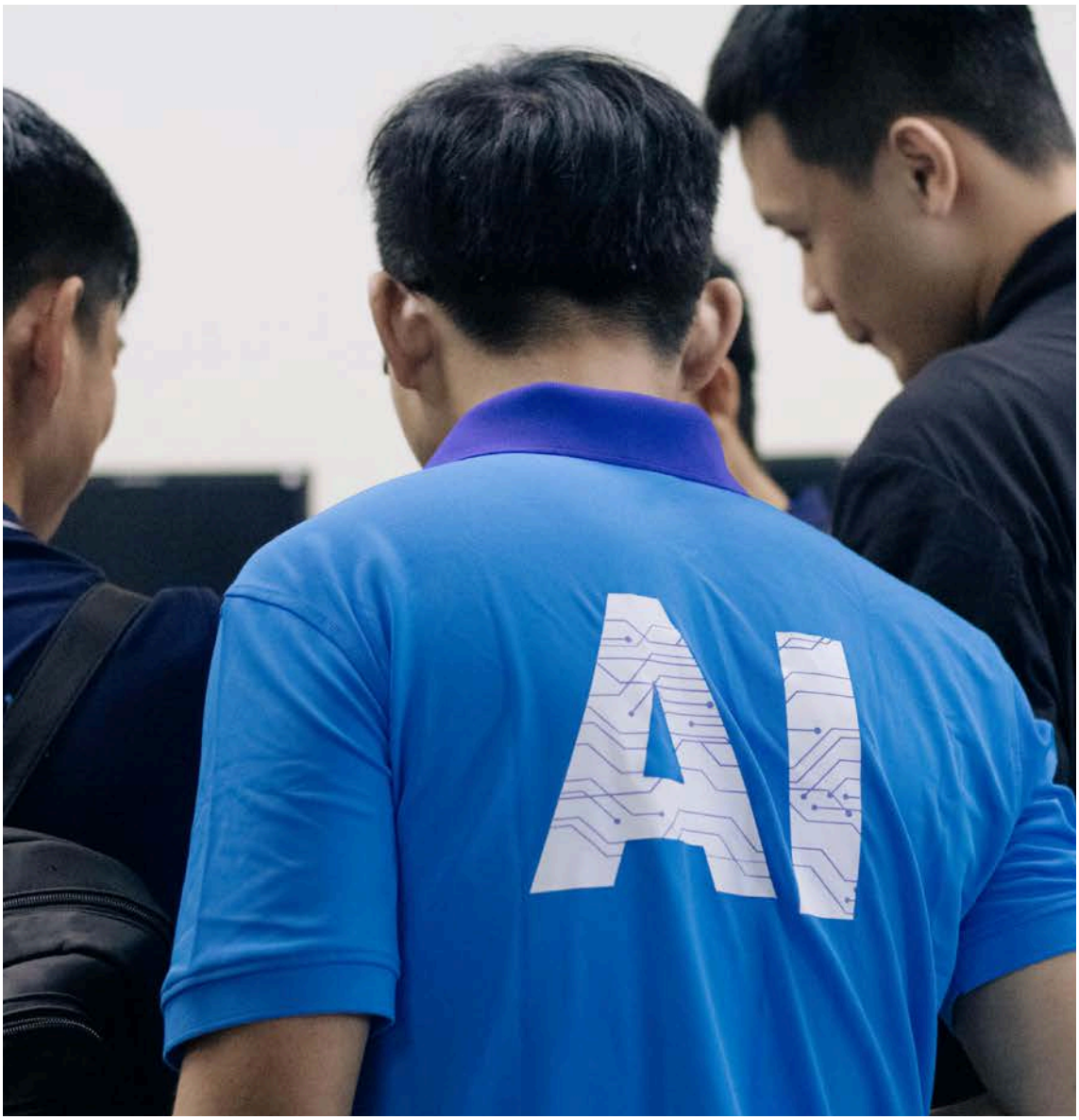
由于NPE本身并不生产或者销售任何专利产品，导致被告无法在诉讼中提出反诉或交叉许可的谈判，丧失了在诉讼中的平衡地位；NPE因此可以利用专利侵权诉讼高成本、高风险、高度复杂等特性来威胁被诉企业以攫取高昂和解费和许可费等，威逼被告公司以维护公司利益等目考虑向其妥协，因此可能会构成专利权滥用。对于滥用权利而提起诉讼的NPE，该《批复》给被诉企业带来了新的应对方式，增加了NPE诉前评估成本和参与诉讼的成本，必将给NPE带来更大的诉讼压力。

结语

从智能手机、人脸识别到无人驾驶等等，人工智能已经渗透到了生活的方方面面。人工智能领域是当前各国政府以及各大型企业博弈的主要战场，人工智能领域技术的发展以及相关专利的积累也必然日新月异；而基于人工智能领域专利诉讼的特点，其也必将成为NPE诉讼的沃土。本文梳理了人工智能领域侵权诉讼的难点以及NPE诉讼的特点，就人工智能领域NPE的威胁与应对进行了初步探讨，希望能够对人工智能领域相关公司起到一定的引导和借鉴作用。

顾萍
合伙人
知识产权部
北京办公室
+86 10 5957 2089
guping@zhonglun.com

贾媛媛
非权益合伙人
知识产权部
北京办公室
+86 10 5957 2342
jiayuanyuan@zhonglun.com



人工智能领域的知识产权许可问题

作者/顾萍、贾媛媛、马超、徐婧妍

通常而言，知识产权的权利人可以通过开发产品、出售复制品等方式利用知识产权为自己带来收益。同时，知识产权权利人许可其他主体一项知识产权的使用权以获得收益也是一种常见的获利方法。

知识产权许可按照对被许可方的约束程度主要可以分为三类：独占许可、排他许可和普通许可。许可人可以是知识产权的所有人，也可以是通过协议等方式获取了许可他人之权利的主体。被许可人被许可的内容则比较多样化，可以是制造、销售包含该知识产权的产品或依据授权向侵权人索赔（即被许可以诉权，常见于涉外诉讼和NPE相关诉讼）等。在不违反法律法规的情况下，专利、著作权、商业秘密和以其他形式体现的，或其他种类的知识产权都可以成为知识产权许可的客体。

许可一般采取书面合同的形式，合同一般会对许可的适用主体、许可类型、时间区间、地域限制、许可费以及争议解决机制等方面进行约定。鉴于许可协议涉及的知识产权的性质，许可协议也常包含保密条款。对于AI技术而言，其自身的特性也决定了与其相关的许可协议往往涉及更多方面的考量。

PART 01
AI知识产权许可特点

首先，AI的行业特性造成了其许可主体和许可方式具备一定特殊性。一般而言，AI领域的主要玩家包括算法方（顾名思义，其负责提供算法）、模型训练方（负责用数据训练模型）、数据方（负责提供数据）和模型使用方（负责最终应用，一般会具体到行业）。由此可见，参与AI开发和使用的主体比较复杂，这也造成了相关许可的复杂化，即在不同主体间且依实际需要的不同，可能出现双向许可、单向许可、再许可等许可方式。对于不断自我发展的AI技术来说，许可范围的划分也是一个重点和难点。此外，AI领域还经常涉及AI平台，即开发者可以通过该AI平台用数据训练其所需的模型，这种情况下的许可协议通常为固定模板。平台方应注意协议模板的合规性、周延性以及免责方面，而用户则应仔细阅读相关条款以避免自身模型出现权利瑕疵。

其次，AI知识产权许可涉及的知识产权多样，可能包括专利、软件著作权、商业秘密和数据利益（可能与商业秘密存在一定程度的重合）等。AI领域按照产业架构一般可以分为基础层、技术层和应用层。对于基础层（提供算力支持），例如AI硬件方面，可以使用专利结合商业秘密来保护知识产权；对于技术层（算法和算法平台），多以商业秘密结合软件著作权保护；对于应用

层（即在各行业中的具体应用），则可通过专利、软件著作权和商业秘密保护知识产权。AI知识产权的类型多样性造成许可时需要兼顾不同类型的知识产权的特点，有针对性地采用适当的许可条款。例如，商业秘密许可会要求严格的保密，而纯专利许可因其公开属性则一般无此要求。又比如，商业秘密的保护期限是永久直至被公众所知悉，专利则为10年至20年不等，著作权保护期则为作者终生及去世后50年（如果为法人作者，则保护期为首次发表后50年），这无疑会影响许可期限的约定。再者，由于专利无效程序的存在，较之其他类型的知识产权，其效力在许可期限内可能会发生变化，因此也需进行有针对性的约定。

再者，人工智能的开发往往一般都需要数据支持。因此，AI知识产权许可还要额外注意数据收集和使用的合规问题，这就要求对于数据合规，各方需要明确各自需承担的义务。例如，一般而言，数据方应确保数据的收集获得了相应许可并且有权授权其他合作方使用；而数据使用方（例如模型训练方）则应承担确保数据的合法使用以及不得泄露等义务。

PART 02

AI知识产权许可改进知识产权权属

“知识产权改进”指的是知识产权许可协议的任何一方对于许可协议中的背景技术进行的性能、效率、功能、成本、应用范围等方面的修改、提升、修正或增强。许可人可能在许可协议期间对背景知识产权进行改进，而被许可人在使用许可过程中也可能对技术做出适应性或创造性的修改。因此，一般要在许可协议中约定此等改进的归属及对价。根据我国法律规定，技术改进的权属优先适用双方合同约定，但在不同情形下的条款约定可能因违反具体适用法域的法律规定而有效力瑕疵。以下将针对不同开发模式下的许可合同条款及其效力加以分析：

2.1 约定一方所有

如果许可合同约定在合同有效期间的知识产权改进的所有权在其产生时即归某一方所有，而无论由合同哪一方开发，则此种模式为一方独有。在实践中，基于双方的谈判地位，约定背景知识产权一方独有的情况并不罕见。但要注意，在不同法域下，该等条款的有效性存疑。例如在欧盟的技术转让集体豁免条例（TTBER）框架下，如被许可人对背景知识产权进行了改进，改进的权属自动转让或独家回授给许可方的条款可能是无效的；即使改进

权属的条款不属于上述情况，如果对改进的转让造成了反竞争的效果，那么合法性也存疑。在中国也有类似的效力问题：《民法典》规定“非法垄断技术或者侵害他人技术成果的技术合同无效”；《最高人民法院关于审理技术合同纠纷案件适用法律若干问题的解释》进一步规定“限制当事人一方在合同标的技术基础上进行新的研究开发或者限制其使用所改进的技术，或者双方交换改进技术的条件不对等，包括要求一方将其自行改进的技术无偿提供给对方、非互惠性转让给对方、无偿独占或者共享该改进技术的知识产权”的，属于“非法垄断技术”。在此种情况下，如果改进是基于背景知识产权，但又由非背景知识产权所有方独立开发，则可能因构成“要求一方将其自行改进的技术无偿提供给对方、非互惠性转让给对方”而被认定为有非法垄断效果。但是，如能证明独立研发方已经获得了合理对价或其开发过程并非完全独立，则该等条款的效力风险依然可控。

2.2 约定共有

如果许可合同约定知识产权改进的所有权在其产生时即归合同各方共同所有，而不论由哪一方开发，此种模式为共同拥有。在此种情况下，应特别注意在特定法域中，知识产权的实施是否反因共同拥有的模式而受到阻碍。例如，在美国法下，如某一专利权人因他人侵犯专利权而诉诸法院，那么所有专利权人都应加入该等诉讼，否则程序无法进行；如被授予改进知识产权归属的某一方怠于加入对知识产权的保护行动，那么共同所有的模式反而不利于改进技术的保护。

2.3 约定实际改进方所有

许可合同也可规定根据实际开发情况而决定对改进知识产权的独有或共有。例如，许可合同可能规定，如由一方独立开发改进的知识产权，该等知识产权的所有权利、所有权和利益归于该开发方；而如由合同多方共同开发，则由多方共同拥有。在条款的有效性上，这样的约定通常并无明显法律瑕疵。只是对于非背景知识产权所有方来说，在与许可方产生争议时，要证明其“独立”开发了基于许可合同背景知识产权的难度较大。此外，对于被许可方来说，需要从商业角度进一步评估此等条款对于许可费用的影响。例如，许可方通常更容易基于现有技术进行改进，并依据此等条款拥有改进技术的所有权。当被许可标的物版本更新迭代较快时，一旦许可方发明了新的版本（例如软件），被许可方就会陷入或者选择额外签署新版本许可合同，或者被新市场淘汰的被动境地。

2.4 改进权属非共有下的许可

值得注意的是，在许可协议下，一般对改进技术不拥有权属的一方可获得对于改进技术的使用许可，而该许可是否免费则视具体情况而有所不同。如果双方就改进技术的许可是否应免费而僵持不下，不拥有权属的一方可以要求以付费方式获得许可的选择权。

PART 03

AI知识产权许可之保证条款

3.1 知识产权不侵权保证

知识产权不侵权保证条款是知识产权许可中的常见条款，其内容包括就被许可的知识产权之使用不侵犯第三方知识产权作出保证。根据许可人和被许可人间的谈判实力对比和其他因素，许可条款中常见的情形有：保证不侵犯第三方知识产权、明确排除不侵权保证、以及不提及知识产权不侵权保证。对于第三种情形，即不提及是否保证不侵犯第三方知识产权的情形，一般认为许可方没有默认的保证义务。因此作为被许可方，应尽量要求许可方作出不侵权保证，以维护自身权利。

3.2 不起诉保证

知识产权许可协议中有时还会包括不予起诉保证，即许可方保证不会起诉被许可方侵犯被许可之知识产权。一方面，这是从许可的反向进行约定，给与许可双保险。在许可本身因为技术出口等限制归于无效时，拥有不起诉保证的被许可方尚存一定的转圜余地。另一方面，是保证许可产品不涉及其他未许可知识产权，或即使涉及也不会面临起诉风险。一般而言，获得许可后不被许可方起诉侵犯知识产权是被许可方基本的诉求，因此建议被许可方尽量要求加入此等条款。

3.3 知识产权有效性保证

毋庸置疑，知识产权许可的基础是知识产权，因此知识产权的有效性必然会对知识产权许可产生实质性影响。根据许可人和被许可人间的谈判实力对比和其他因素，许可条款中常见的情形有：保证知识产权有效性、明确排除对知识产权有效性的保证、以及不提及对知识产权有效性的保证。明确排除对知识产权有效性的保证常见于“技术包许可”的情形，其目的在于不因部分知识产权的失效而影响许可费率。而在不提及知识产权有效性保证

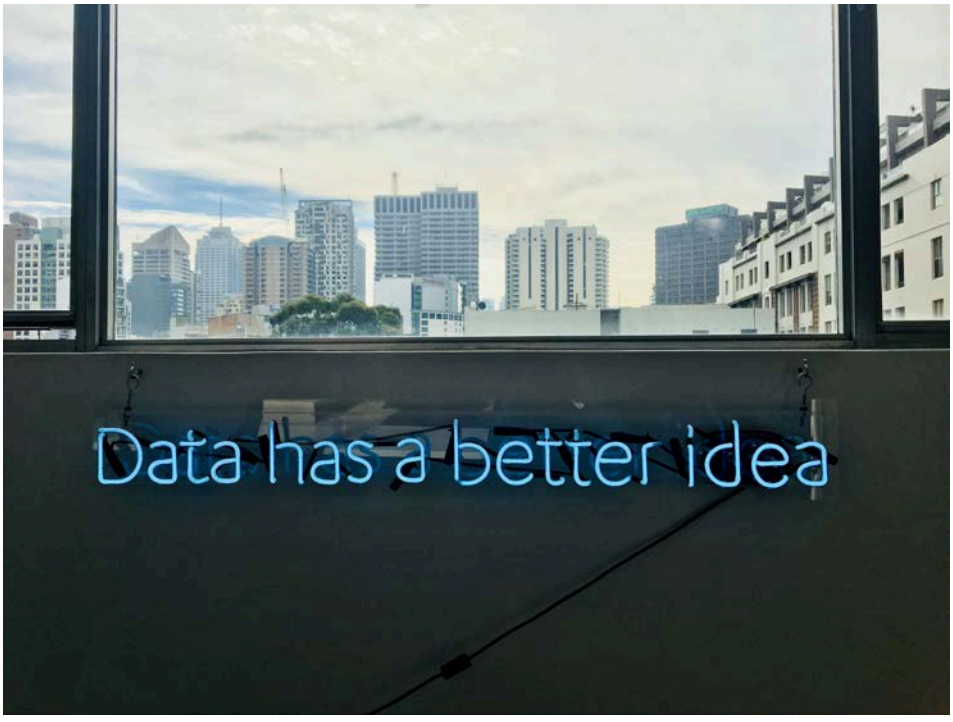
的情况下，如果许可涉及的全部或主要知识产权失效，则被许可方一般可以以此为由，要求减少许可费；如果许可方作出了知识产权有效性保证，则更是如此。

3.4 技术有效性保证

技术有效性保证即许可方对被许可方作出许可技术能够实现协议目的之保证。基于许可方和被许可方谈判实力对比和其他因素，知识产权许可中对于技术有效性的保证会有三种情形：保证技术有效、不提及技术有效性保证、和明确排除对于技术有效性的保证。对于AI平台，因开发应用的不确定性较高，对于许可方来说，一般建议明确排除技术有效性保证。

3.5 人身、财产损害赔偿保证

对于AI应用的部分领域，如自动驾驶等，还可能由于AI的运用而导致对人身、财产的损害。因此，有必要在许可合同中明确许可方是否承担相应责任。对于此等类型的保证，许可方明确不承担相关赔偿责任或者对相关赔偿责任作出明确限制是较为常见的情形。



PART 04

AI知识产权许可不挑战条款

知识产权许可合同中的不挑战条款，顾名思义，即要求被许可方不得挑战许可知识产权的效力，其形式上通常有两种：

（1）直接禁止被许可方对于许可知识产权提出挑战，例如提起专利无效程序或主张其无效等；

（2）如另一方对于提供知识产权一方提出现有知识产权挑战，则许可合同可由许可方终止。

不论是上述哪一种方式，其从实质上都构成了对被许可人挑战相关知识产权的限制，因此有可能因构成非法垄断技术而造成该条款无效。

《民法典》第八百五十条规定："非法垄断技术或者侵害他人技术成果的技术合同无效"。《最高人民法院关于审理技术合同纠纷案件适用法律若干问题的解释》进一步规定："非法垄断技术"包括"禁止技术接受方对合同标的技术知识产权的有效性提出异议或者对提出异议附加条件"的情形。因此，在中国，此等不挑战条款有效性存疑。

在美国，案例法曾判定，诉讼前的许可协议中此等条款无效。因此可能导致被许可人一方面有权利挑战相关知识产权的有效性或可执行性，另一方面在支付许可费的情况下仍可享受许可协议项下的权利，或被许可人也可以选择停止支付许可费；但如果在诉讼提起后，双方签订的和解协议内含许可及不挑战条款，那么该等条款有效性取决于诉讼案件进展的情况，双方的证据开示越充分，则条款有效的可能性越高。在欧盟，《欧洲联盟运作条约》和《技术转让集中豁免》（TTBE）也有类似反垄断的规定。因此，许可双方应基于许可合同类型、双方市场地位、许可有偿性、技术新颖性、是否涉及特定知识产权（如标准必要专利）等方面特别注意该等条款的有效性。此外，建议许可双方在协议中纳入"分割性"条款，保证不挑战条款的无效不影响其他条款效力。

除了不挑战条款以外，双方也可以考虑以下替代方案，以起到防止被许可方无端提出对知识产权挑战的作用：

①调整许可费的安排，例如要求被许可人在许可期间一开始即支付大部分费用，或规定在被许可人挑战知识产权时许可费用将自动提高；

②不设定固定长期的许可期限，对于许可期限规定为可延长的短期有效期，且双方都可在本期到期之前提出终止合同；

③约定许可可能因被许可人提出知识产权挑战而降级（例如由独占许可

转为普通许可）；

④约定被许可人应支付许可人应对专利无效挑战所产生的律师费和其他成本；

⑤约定被许可人在挑战知识产权有效性之前需提前通知许可人，以便许可人及时应对。

PART 05

AI知识产权许可合规义务

对于数据合规，在文集第二章中有详细讨论，本节将主要强调合规责任的分配问题。如前所述，对于AI知识产权许可而言，大原则是：数据方应确保数据的收集获得了相应许可并且有权授权其他合作方使用；而数据使用方（例如模型训练方）则应承担确保数据的合法使用以及不得泄露等义务，即各方应保证在自身可控制的范围内的合法合规。虽然通过协议可以就各方责任予以明确划分，但是作为参与AI项目的各方可能仍需要承担基本的审查义务，该等义务不一定能被协议约定所免除，即参与人工智能项目的一方可能被违规收集或使用数据的另一方“牵连”。因此，为控制自身合规风险，建议对合作伙伴的资质进行形式审查，请合作伙伴对于数据收集过程合规或数据使用合规作出保证，并且在协议中约定数据不合规时的违约责任，以最大限度规避自身风险。

PART 06

AI知识产权许可防止非法移植

基于AI知识产权的特点，非法移植是AI知识产权许可的一个重点和难点。此处的非法移植指被许可人（例如模型训练方或模型使用方）擅自对作为合作成果的模型进行调整，而用于许可外的其他客户或领域的情况。此等情况较难证明，但又比较容易发生，因此是AI知识产权许可需要重点防范的风险之一。而作为应对方法，可以尝试从两个途径入手：

6.1 技术手段

AI往往涉及软件，而软件可以一些比较成熟的手段进行管控。作为使用限制，软件可以施加秘钥，从而达到每台设备上使用软件均需要权利人授权的目的。秘钥本身可以采用数字和硬件的方式。另一方面，为了降低举证难

度，权利人可以在软件中加入无意义代码段作为一种“签名”，从而便于初步证明软件的真实来源。

6.2法律手段

对于非法移植的问题，也可以采用协议约定的方式尝试解决权利人举证困难的问题。例如，可以约定对于是否存在非法移植一事适用举证责任倒置。所谓举证责任倒置，指本来应当配置给一方当事人的举证责任转移给另一方当事人承担。针对当前所述情形，可以在许可协议中约定，在未获得许可方许可的情况下，一旦许可方发现被许可人的客户使用了与合作开发项目类似功能的AI产品/服务，则被许可方应举证证明该等AI产品/服务与许可的知识产权无关，但被许可方拥有对模型完全处置权（包括再许可权）的除外。

结语

如前文所述，AI行业中，由于涉及到的开发和使用的主体比较复杂，技术不断革新，并且很有可能涉及到平台间的交互，AI行业的许可主体和许可方式相对来说更具复杂性和特殊性。各方应当注意知识产权许可项下可能触发的问题，仔细审慎约定相关条款，以有效规避风险，节约成本。

顾萍
合伙人
知识产权部
北京办公室
+86 10 5957 2089
guping@zhonglun.com

贾媛媛
非权益合伙人
知识产权部
北京办公室
+86 10 5957 2342
jiayuanyuan@zhonglun.com

人工智能领域商业秘密管理

作者/陈际红、蔡鹏

人工智能属于新兴的高科技行业，能够以科技赋能各行各业，在市场上亦存有无限商机。全球范围内的相关企业均在该领域中投入了大量的研发资源，已经存在，且即将可能产生大量具有高商业价值的技术秘密/经营秘密。然而，实践中稀缺人才的频繁流动势必可能会带来商业秘密的泄露危机，加之竞争企业往往会进行商业秘密上的刺探、运用黑客技术窃取商业秘密、内部员工被引诱/不慎/甚至故意泄露商业秘密等各种因素，使得人工智能领域的高新技术企业往往面临着非常大的商业秘密被侵犯的风险。对于人工智能企业来说，商业秘密的保护在其知识产权保护布局中，应当占据较大的比重。

PART 01

中国商业秘密保护的立法和司法动态

虽然2021年1月1日生效的《民法典》第一百二十三条明确将商业秘密纳入知识产权的范围，但从我国现有立法来看，侵害商业秘密的行为仍列为不正当竞争行为。在司法实践中，对侵害商业秘密行为的救济，主要依据的是2019年修订的《中华人民共和国反不正当竞争法》（以下简称“**《反不正当竞争法》**”）第九条，以及《中华人民共和国刑法》（以下简称“**《刑法》**”）第二百一十九条规定的侵犯商业秘密罪。

其中，《反不正当竞争法》在2019年4月23日修订并实施，主要涉及以下方面的变化：

1.进一步完善了商业秘密的定义，明确了侵犯商业秘密的情形，即在第九条第三款中将“本法所称的商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息和经营信息”修改为“本法所称的商业秘密，是指不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。”，在第九条第一款第（一）项中增加了“电子侵入”手段，第（三）项中用“违反保密义务”替换原先的“违反约定”，新增第（四）项中“教唆、引诱、帮助”侵犯商业秘密的情形；

2.扩大了侵犯商业秘密责任主体的范围，即新增第九条第二款将经营者以外的其他自然人、法人和非法人组织纳入侵犯商业秘密责任主体的范围；

3.强化了侵犯商业秘密行为的法律责任，即在第十七条中引入惩罚赔偿规则，对于恶意实施侵犯商业秘密行为，情节严重的，按照实际损失或侵权获益的1~5倍确定赔偿数额；第二十一条增加了“没收违法所得”，并将不同

严重程度下的行政罚款分别提升至“一百万元”和“五百万元”；

4.对侵犯商业秘密的民事审判程序中举证义务的转移作出了规定，即在第三十二条中新增商业秘密权利人提供初步证据商业秘密被侵犯的情况下，涉嫌侵权人应当证明权利人所主张的商业秘密不属于本法规定的商业秘密。

自《反不正当竞争法》2019年修订并实施以来，有关商业秘密的立法和司法在2020年呈现出一些新的变化，主要包括：

◆2020年1月15日中美双方在美国华盛顿签署的《中华人民共和国政府和美利坚合众国政府经济贸易协议》中关于商业秘密相关内容的部分；

◆2020年9月12日起施行的《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》；

◆2020年9月14日起施行的《最高人民法院、最高人民检察院关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》；

◆2020年9月17日最高人民检察院、公安部《关于修改侵犯商业秘密刑事案件立案追诉标准的决定》。

2020年最新的立法和司法动态，以及相关的内容变化概述如下表1所示。

时间节点	重要事件
2020年1月15日《中华人民共和国政府和美利坚合众国政府经济贸易协议》（简称“中美经贸协定”）	中美经贸协定在开篇部分（第一章 知识产权 第二节 商业秘密和保密商务信息）特别关注到商业秘密的保护问题，即重点约定以下内容： 第1.3条中明确了侵犯商业秘密责任人的范围； 第1.4条中在构成侵犯商业秘密的禁止行为范围中增加了“电子入侵”、“违反或诱导违反”以及“有义务保护商业秘密”。 第1.5条中要求中国应规定商业秘密案件民事程序中举证责任转移的条款和相关情形。 第1.6条中的阻止使用商业秘密的临时措施中要求中国“紧急情况”司法机关有权采取行为保全措施。 第1.7条 的启动刑事执法的门槛中要求中国 “重大损失”可以由补救成本充分证明，并应显著降低启动刑事执法的所有门槛。 第1.8条中提到刑事程序和处罚， 第1.9条中提到保护商业秘密和保密商务信息免于政府机构未经授权的披露的情形。
2020年9月12日，最高人民法院发布了《关于审理侵犯商业秘密民事案件适用法律	在商业秘密的民事保护方面，尤其需要关注的是，最高院在《2020商业秘密民事案件若干规定》中对商业秘密的保护客体（包括技术信息、经营信息、客户信息的界定）、商业秘密的构成要件（包括“非公知性”标准、“保密性”

时间节点	重要事件
若干问题的规定》（简称“《2020商业秘密民事案件若干规定》”）	标准、“商业价值”范围）、侵权行为方式（包括获取、使用、反向工程、员工和前员工的界定、模式保密义务、实质相同的判定标准）、民事诉讼程序安排（包括保全措施）、民事责任体系（停止侵害的期限、返还载体和消除信息、认定赔偿数额的各种考量因素、商业价值的考量因素、商业秘密许可使用费的考量因素、参照刑事判决认定赔偿、侵权人不提供侵权赔偿证据情况下的赔偿认定方式）、刑民交叉的处理（包括调查取证、侵权损害赔偿认定、中止审理情形）等方面都进行了更为细致和明确的规定，为统一商业秘密民事案件的审理尺度提供了审判标准，也为企业在商业秘密方面的合规工作提供了可操作化的重要指引。
2020年9月12日，最高人民法院、最高人民检察院发布了《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》，并于2020年9月14日起实施。 2020年9月17日，最高人民检察院、公安部发布了《关于修改侵犯商业秘密刑事案件立案追诉标准的决定》，并于发布日期开始实施。	基于2020年9月最高人民法院、最高人民检察院、公安部先后发布的相关司法解释和决定，启动刑事执法的门槛明显降低（由五十万元降低为三十万元），扩大了侵犯商业秘密入罪行为的范围，并且对损失数额或者违法所得数额的计算方式给出了更为详细的规定和指引。 尤其需要关注的是，为了响应中美经济贸易协定，相关解释和决定还将商业秘密的权利人为减轻对商业运营、商业计划的损失或者重新恢复计算机信息系统安全、其他系统安全而支出的补救费用计入给商业秘密的权利人造成的损失，这使得在侵权数额的认定上有更宽泛的计量标准，使得商业秘密的刑事违法成本更高。

从上表可以看出，中美经济贸易协定中关于商业秘密的约定内容基本都体现在了后续《2020商业秘密民事案件若干规定》《关于办理侵犯知识产权刑事案件具体应用法律若干问题的解释（三）》等文件中，特别是关于保全措施、举证责任转移、以及降低刑事执法的门槛的相关条款内容。

PART 02

商业秘密修法后对人工智能行业的影响

经历了本年度商业秘密修法之后，中国在商业秘密保护上日趋严格。目前来看，商业秘密修法对人工智能行业的影响主要体现在以下几个方面：

1、商业秘密保护客体的变化有利于人工智能行业的发展

2019年《反不正当竞争法》修改之后，将商业秘密的保护客体扩展为“技术信息、经营信息等商业信息”，实践中对“技术信息”和“经营信息”的理解一直存在偏差，本次《2020商业秘密民事案件若干规定》中明确地给出了“技术信息”和“经营信息”的具体定义，对此予以了明确。

对于人工智能行业而言，技术秘密和经营秘密等商业信息对企业的发展都至关重要，因此将此类信息都纳入商业秘密的保护客体范畴，有利于促进人工智能行业的成长和发展。此外，本次修改明确将生产经营活动中形成的阶段性成果在符合相关规定的情况下也纳入商业秘密的范畴，进一步扩展了保护客体，有助于对实际中较为常见的研发或交易过程中产生的阶段性成果进行商业秘密保护。

2、源代码、算法、数据及其有关文档都属于技术信息

在技术信息的定义方面，本次《2020商业秘密民事案件若干规定》中明确地将算法、数据、计算机程序及其有关文档纳入技术信息的范畴，有助于涉软件行业（包括人工智能）的商业秘密保护。在计算机程序方面，传统意义上是将其作为著作权保护或专利权保护的客体，由于计算机程序的无形性、鉴定难度较高等因素的影响，涉软件的商业秘密保护力度相对较弱。

人工智能领域经常会涉及神经网络、样本训练、大数据处理、计算机视觉、语音识别等算法、数据及其相关软件的改进，因此，目前修法之后将源代码、算法、数据及其有关文档都明确为技术秘密，势必为企业在涉软件商业秘密的保护方面提供强有力的法律依据，也体现了鼓励该等领域商业秘密保护的司法趋势。

3、举证妨碍制度和惩罚性赔偿制度有利于人工智能企业合法维权

商业秘密维权存在举证难的顽疾，本次修法之后在此问题上实现了一定的突破，也即在《2020商业秘密民事案件若干规定》第二十四条中引入了举证妨碍制度，即在权利人已经提供了侵权人因侵权所获得利益的初步证据的情况下，但与侵犯商业秘密行为相关的账簿、资料由侵权人掌握的，人民法院可以根据权利人的申请，责令侵权人提供该账簿、资料。侵权人无正当理由拒不提供或者不如实提供的，人民法院可以根据权利人的主张和提供的证据认定侵权人因侵权所获得的利益。

在商业秘密领域中，侵权获益的真实数据通常掌握在被告一方，原告通常只能从外围获得初步的证据（甚至只能通过评估鉴定报告来进行估计），

难以获得高额的侵权赔偿。因此，举证妨碍制度的引入为商业秘密权利人获得高额赔偿、维护自身合法权益打开了一扇窗。此外，2019年修订的《反不正当竞争法》还规定了商业秘密侵权的惩罚性赔偿制度，因此，举证妨碍制度与惩罚性赔偿制度的结合，必将为人工智能企业打击侵权、获得充分赔偿奠定坚实的法律基础。

4、保密措施的明确为人工智能企业构建保密措施体系提供了指引

商业秘密案件中非常关注秘密性和保密性，《2020商业秘密民事案件若干规定》中强调了保密措施必须在被诉侵权行为发生前采取，才能构成反不正当竞争法下的“保密措施”，这对企业在商业秘密方面的保密措施设置了时间上的门槛。

而在保密措施的判断标准上，需要根据商业秘密及其载体的性质、商业秘密的商业价值、保密措施的可识别程度、保密措施与商业秘密的对应程度以及权利人的保密意愿等因素来进行综合判断。最高法列举了常见的保密措施，包括签订保密协议、限制生产经营场所的访问、对商业秘密及其载体进行区分管理、对计算机设备等采取禁止或限制访问、要求离职员工返还商业秘密和载体等合理的保密措施。因此，对于人工智能行业的企业而言，可以参照以上保密措施的时间门槛和具体措施判断标准来构建良好的保密措施体系，从而加强商业秘密的保护，也方便后续在可能发生侵权纠纷时通过举证来保护自身权益。

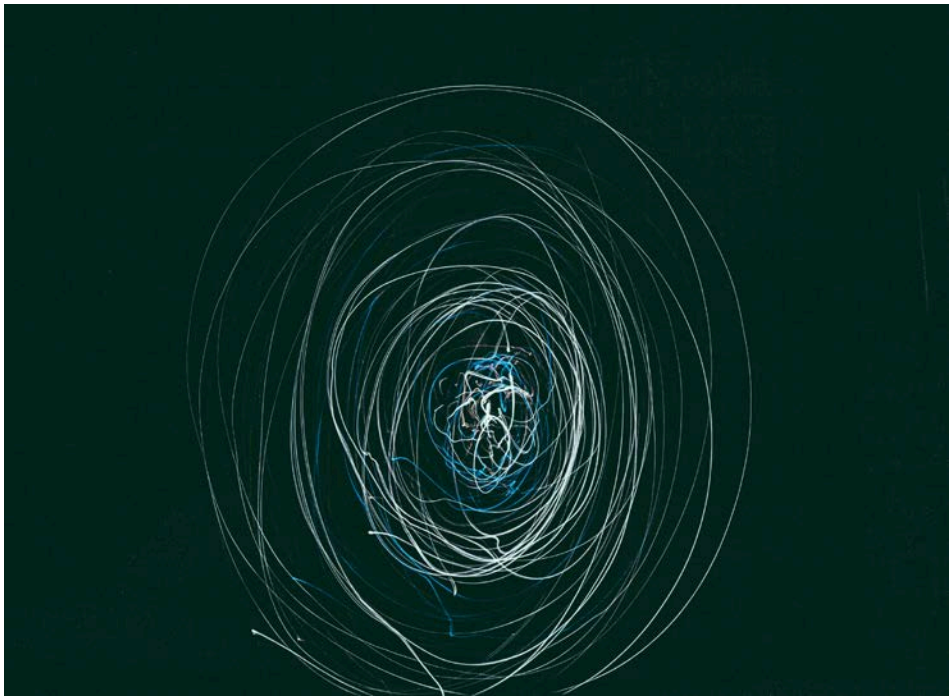
5、员工跳槽所带来的商业秘密侵权风险仍需人工智能企业重点关注

《2020商业秘密民事案件若干规定》第十一条、第十二条等条款对员工、前员工的身份认定及其接触行为进行了明确，与企业具有劳动关系的人员都会被纳入侵犯商业秘密的主体的范畴，而该等员工由于职务、职责、权限关系接触到商业秘密的行为都会在判断“接触+实质性相似”时予以综合考虑。

以上修法一方面为人工智能企业规制员工/前员工的商业秘密侵权行为提供了维权途径，另一方面也为人工智能企业防范由于员工侵犯前雇主的商业秘密而被动卷入纠纷的合规义务提出了更高的要求。

6、赔偿标准的清晰有利于人工智能企业商业秘密的保护

《2020商业秘密民事案件若干规定》第十九条、第二十条对《反不正当竞



争法》第十七条的赔偿事宜进行了进一步明确，包括：因侵权行为导致商业秘密为公众所知悉的，在确定赔偿数额时可以考虑商业秘密的商业价值，包括研究开发成本、实施该项商业秘密的收益、可得利益、可保持竞争优势的时间等因素；在法定赔偿情形下，可以考虑商业秘密的性质、商业价值、研究开发成本、创新程度、能带来的竞争优势以及侵权人的主观过错、侵权行为的性质、情节、后果等因素。

因此，在商业秘密由于侵权而为公众所知悉时，可以引入商业价值的考量因素，将研发成本、收益、可得利益等考虑在内，这为人工智能企业举证侵权损失提供了证明思路。而在实际损失或侵权获益难以确定时，还可以在法定赔偿情形下综合考虑商业价值、研发成本、创新程度等因素来综合判断，因此企业可以在例如研发过程中保留相关的研发成本证据，以方便在侵权纠纷时提供赔偿证据。

总之，无论是商业秘密的民事保护，还是刑事保护，经过2019年和2020年的立法变化和司法解释的进程之后，中国在商业秘密的全方位保护方面更趋严格，为包括人工智能企业在内的创新主体的商业秘密保护提供了更强有力的法律支撑，但同时也对人工智能企业商业秘密民事和刑事合规方面的工作提出了更高的要求，值得关注。

PART 03

人工智能领域的商业秘密纠纷典型案例

近年来，商业秘密的民事纠纷和刑事纠纷时有发生，经查询“威科先行”数据库，商业秘密的民事纠纷案件共计3960条记录，其中：侵害技术秘密纠纷585件（占比53.77%），侵害经营秘密纠纷449件（占比41.27%），侵犯商业秘密竞业限制纠纷54件（占比4.96%），可见技术秘密纠纷案件比经营秘密纠纷案件占比稍大。商业秘密纠纷案件按审理年份统计如下图1所示，审级和标的额统计如下图2所示。

从图1和图2中可以看出，商业秘密民事纠纷的案件量较多，近三年的案件占比1/3左右，而2017年-2020年的案件占比40%以上，这与我国近年经济快速发展，市场竞争加剧等因素都有关联。而从商业秘密民事纠纷案件的审级上来看，基层法院占比29.44%，中级法院占比43.71%，高级法院占比15.99%，最高法院占比3.84%，可见，中级法院在审理的案件量上占比较多，而目前由于技术秘密纠纷的一审案件基本都由中级法院（包括知识产权法院）来审理，而二审案件会飞跃上诉到最高院，因此在审级上，中级法院和最高院的案件占比可能会进一步增加。

从标的额上来看，10万以下的占比25.51%，10-50万占比36.08%，50-100万占比13.87%，100-500万占比19.34%，500以上的占比5%左右。因此商业秘密民事纠纷近六成案件的标的额在50万以下，50-500万标的额的案件占比30%，相对于其他类型的知识产权案件来说，标的额更高，这可能也与商业秘密案件的侵权后果较严重有较为直接的关联。

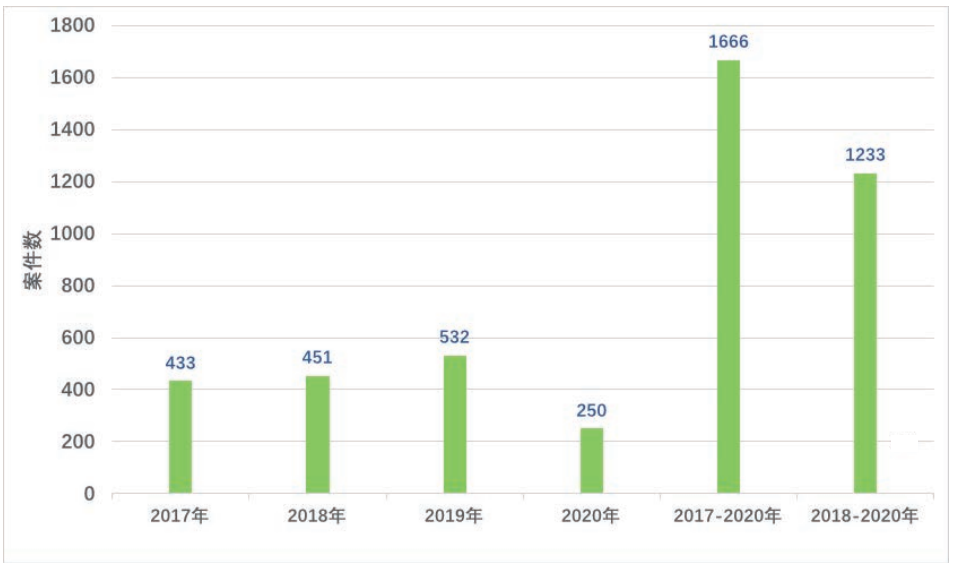


图1 商业秘密民事纠纷统计数据（按审理年份）

图2 商业秘密民事纠纷案件审级和标的额统计

在商业秘密的刑事案件方面，经查询“威科先行”数据库，共计250条结果，商业秘密纠纷案件按审理年份统计如下图3所示，按地域统计如下图4所示。

如图3和图4所示，从案件数量的按年分布来看，分布并不均匀，最近四年的案件量占据20%左右，近三年的案件量占据12%左右，并不能看出商业秘密犯罪的案件量的激烈变化，但随着目前立法和司法中将商业秘密犯罪的入刑标准从50万降低为30万，并且扩大了侵权行为的范围，可能会在以后数年中出现案件量增长的情况。

从案件的地域分布来看，广东占比21.1%，浙江占比16.46%，江苏占比11.81%，上海占比9.7%，北京占比9.7%，可以看出商业秘密的刑事犯罪高发于经济发达的省份和直辖市，这与相关高新技术企业集中在这些区域中密切关联。从审级上来说，据统计，侵犯商业秘密的犯罪案件审理方面，基层法院占比44.4%，中级法院占比46.8%，高级法院占比7.6%，最高法院占比0.4%，由此可见，基层法院和中级法院主要承担了商业秘密犯罪的一审和二审工作，这与刑事案件的立案、侦查、管辖等相关法律规定有关。

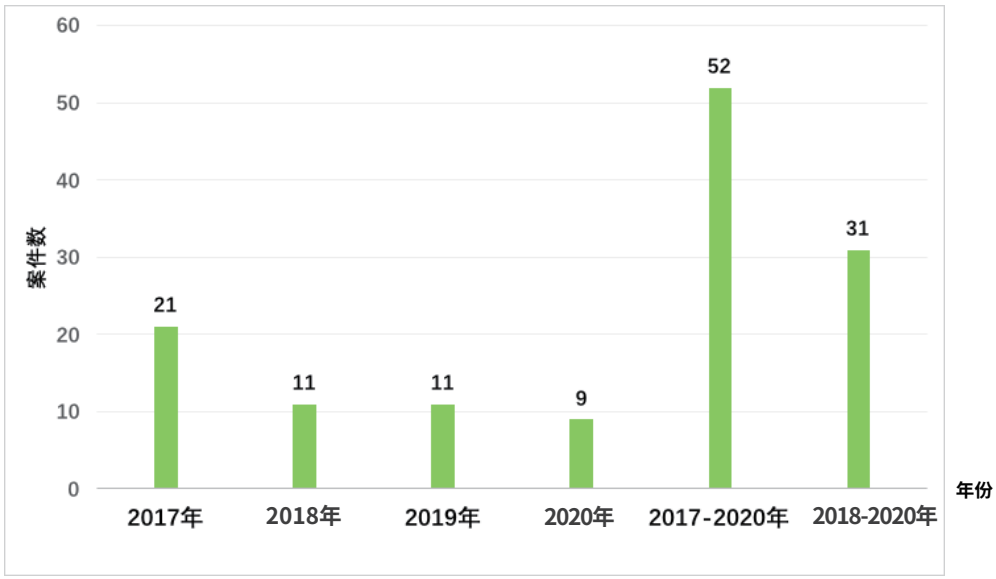


图3 商业秘密刑事案件统计数据(按年)

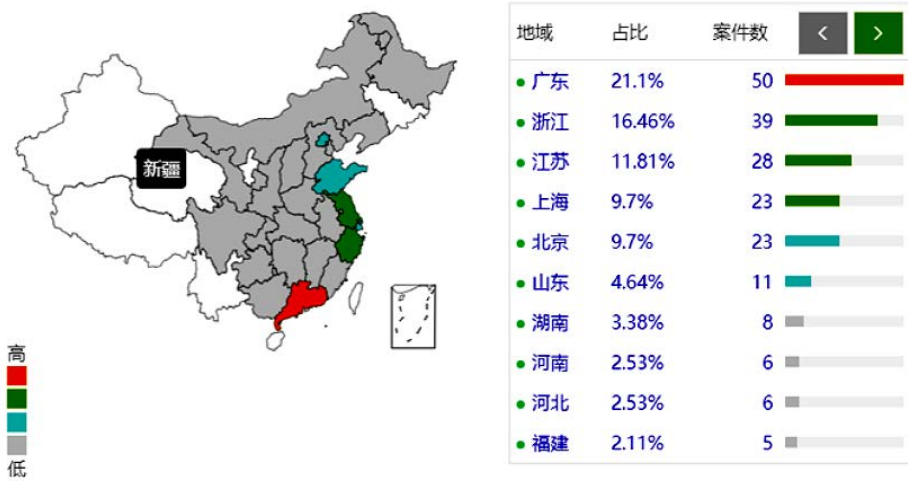


图4 商业秘密刑事案件地域统计数据

近年来在全球人工智能领域发生的影响力较大的商业秘密民事和刑事案件,归纳如下表2所示。

企业名称	争议对方	涉案金额	争议内容
某无人驾驶技术公司	某科技公司	2.45亿美元	某无人驾驶技术公司将某科技公司告上法庭，指控其通过收购前者离职工程师L的无人驾驶公司，盗窃其无人驾驶技术。据称，某科技公司在聘用L时，知道或应当知道其拥有超过1.4万份可能涉及到知识产权的机密文件，L在离职前夕从公司电脑上下载了大量的机密文档。最终，某科技公司以约0.34%的股份（约2.45亿美元）换取了某无人驾驶技术公司的撤诉及和解，二者持续近一年之久的侵犯商业秘密之争宣告结束。
Title Source公司	House Canary公司	7.4亿美元	2016年4月，HouseCanary（一家专注于住宅房地产数据和分析的硅谷公司）基于其拥有与AVM（自动化评估模型，是采用人工智能（AI）并用于评估贷款决策的财产价值的计算机模型）相关的商业秘密的主张，在与Title Source的合同纠纷中提出Counterclaim，认为其违反德克萨斯州《统一商业秘密法》（“TUTSA”）盗用其商业秘密，欺诈和违反合同。2018年3月，陪审团判给House Canary 7.06亿美元赔偿金，包括2.354亿美元补偿性赔偿金和4.714亿美元惩罚性赔偿金。
百度公司	王某	5000万	2017年12月22日，百度以侵犯商业秘密为由，将其百度前自动驾驶事业部总经理王某，和王某离开百度后创立的公司诉至北京知识产权法院。百度在起诉中提到，百度和王某在劳动合同中明确约定了竞业限制义务、不招揽百度员工义务及保密义务，百度还称，王某离职百度前就策划设立公司。该公司自成立以来，一直在中国市场进行业务开拓，在自动驾驶领域与百度具有直接竞争关系。百度提供的一个明确指控是：通过离职不归还电脑和打印机的方式窃取公司机密。2019年5月7日法院对此案进行了不公开开庭审理，在案件审理期间，百度于2020年1月10日向法院申请撤回本案诉讼。
大疆公司	前员工	罚金20万并处有期徒刑六个月	2017年安全研究员K在大疆的网络安全方面发现一个漏洞，后续事件的发酵引起了各国媒体轰动，对大疆公司声誉造成一定的负面影响。经过大疆公司的调查，该漏洞是大疆的一名前员工将含有公司农业无人机的管理平台和农机喷洒系统两个模块的代码上传至GitHub网站的“公有仓库”，造成了源代码泄露长达四年之久。经鉴定，大疆这些泄露出去的代码属于商业秘密，并且造成大疆公司经济损失116.4万元人民币。2019年4月，深圳法院对大疆源代码泄露案做出一审判决，综合考虑犯罪情节以及自愿认罪、有悔罪表现，以侵犯商业秘密罪判处大疆前员工有期徒刑六个月，并处罚金20万人民币。

从表中列举的四个典型案例可以看出，人工智能领域的商业秘密相关的民事和刑事案件高发于有竞争关系的企业主体之间（但应注意有合作关系的企业之间也可能会由于合同违约等因素而产生商业秘密纠纷），标的额巨大，而且经常是由于高管/员工的跳槽行为导致商业秘密泄露而产生民事和刑事的严重纠纷。此外实践中由于企业员工不慎或者故意泄密产生的商业秘密纠纷也时有发生，严重时会导致严重的刑事责任。

正如本文开篇所言，人工智能产业发展迅速，市场规模逐年攀升，商业秘密被侵犯风险大。从目前国内外商业秘密的典型案例来看，企业具体可能卷入商业秘密纠纷的时点如下：

◆在创始人创办企业时，可能会存在与创始人前雇主之间的潜在商业秘密侵权风险；

◆在企业招聘员工时，可能会由于员工的不当行为而与该员工的前雇主之间存在潜在商业秘密侵权风险；

◆在与其他企业商业/技术合作时，可能会由于其他企业存在侵犯商业秘密的情形（例如侵犯第三方商业秘密），而卷入侵犯商业秘密的纷争；

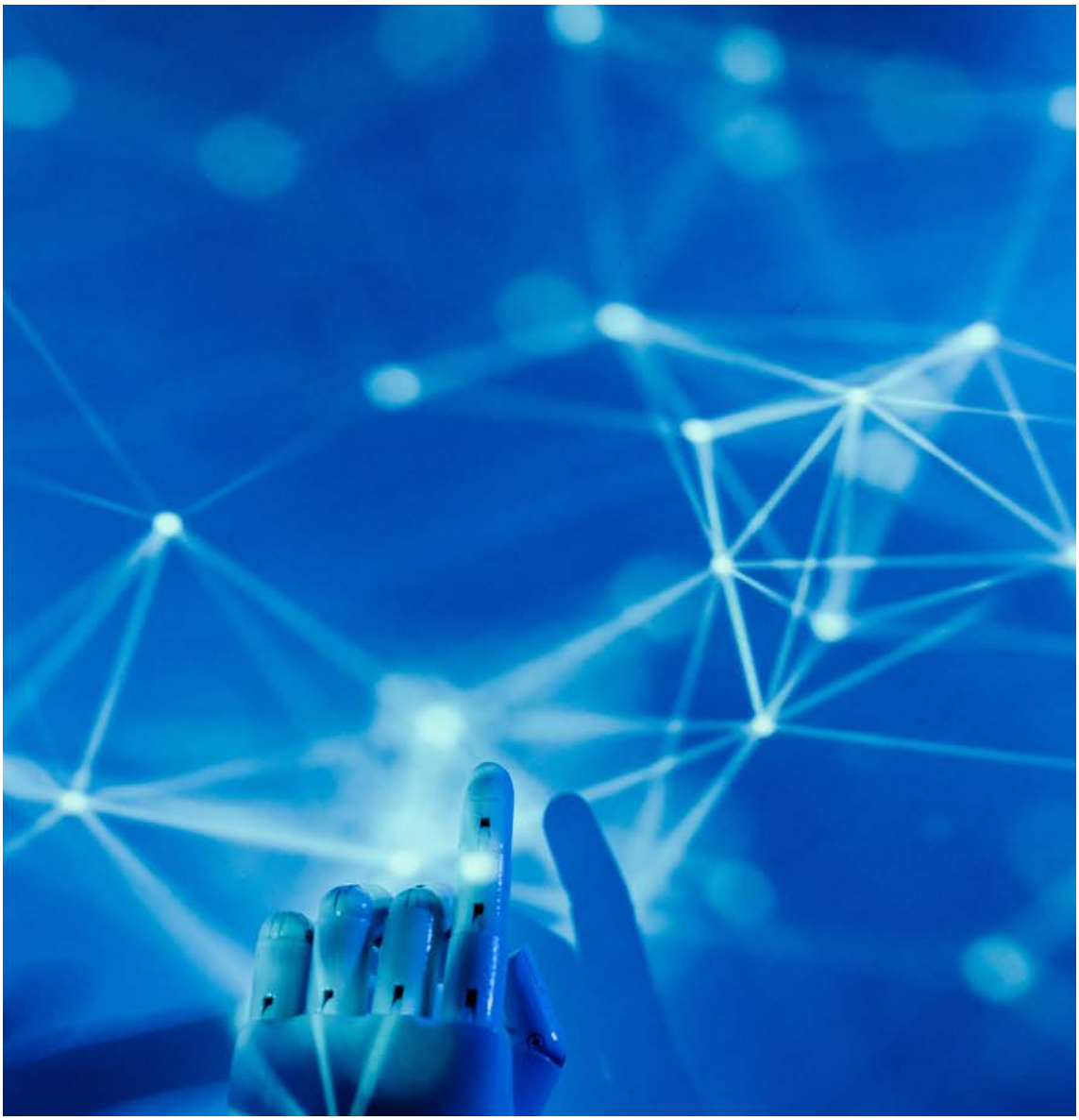
◆当企业的商业秘密保护措施存在漏洞，导致商业秘密不慎泄露、被竞争对手非法获取、或者被员工不慎/甚至故意泄露（例如源代码的泄露）；

◆在员工离职时，由于未能处理好与该员工之间在技术秘密、竞业禁止等方面的关系，而导致与该员工的后续雇主之间产生纠纷。

总之，我们建议企业在不同时点，不同场景，布局相应的商业秘密保护措施。

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

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



人工智能知识产权的司法保护热点问题

作者/王红燕、徐天冉

2012年一家中国人工智能公司（上海智臻智能网络科技有限公司，以下简称“小i机器人公司”）对美国苹果公司在上海第一中级人民法院提起诉讼，指控苹果公司的语音识别技术侵犯了其专利。2020年6月28日，最高人民法院认定小i机器人的专利有效，Siri的技术方案落入了小i机器人ZL200410053749.9号专利权利要求的保护范围。2020年8月3日，小i机器人公司在上海高级人民法院对苹果公司提起了第二次诉讼，要求赔偿100亿元人民币（约14亿美元），并要求苹果公司停止 "制造、使用、承诺销售、销售和进口 "侵犯该专利的产品。

目前，这场诉讼还依然在进行中，可以预见的是，这将又会是一场涉及人工智能专利保护的诉讼持久战。近年来，技术进步带来了生活方式与商业产品的革新，人工智能已被部署在许多场合——从精准广告投放到自动驾驶汽车，再到AI智能合同与文件审查，人工智能技术每天都在影响着大众生活。无论是头部互联网企业、上市科技公司还是初创科技企业，都在不断向人工智能领域投放大量资金，并在人工智能技术研发、推广上耗费心血。根据权威机构的估算，预计2024年，中国人工智能市场规模将达到172.2亿美元的市场规模。国际数据公司（IDC）与浪潮集团日前联合发布的《2020-2021中国人工智能计算力发展评估报告》预测，2024年中国在全球人工智能市场的占比将达到15.6%，成为全球市场增长的重要驱动力。[1]人工智能在提高社会工作效率的同时，也对我国现有的知识产权保护法律体系和造成一定的冲击和挑战。

1. 新华社：中国将成为全球人工智能市场增长的重要驱动力 http://www.gov-.cn/xin-wen/2020-12/16/-con-tent_5569878.htm 2020-12-16

2.吴汉东、张平、张晓津：”人工智能对知识产权法律保护的挑战“，《中国法律评论》2018年第2期，第59-78页

PART 01
人工智能的概念

什么是人工智能?中国电子技术标准化研究院等单位在2018年编写发布的《人工智能标准化白皮书(2018版)》定义了人工智能是围绕智能活动而构造的人工系统，是知识的工程，是机器模仿人类利用知识完成一定行为的过程。依据人工智能是否能真正实现推理、思考和解决问题，可以将人工智能分为弱人工智能和强人工智能。弱人工智能是不自觉的，没有自主意识的，不能真正做到与人类相同的推理。强人工智能是指有自我意识的，甚至可以拥有人一样的思考和机器专有的跟人类不一样的角度思考的两种能力，强人工智能都达到了能够适应外界环境挑战的一般人类水平。[2]

常见的人工智能应用领域主要集中在应用感知智能技术，例如身份认

证，人脸识别的门禁安保，语音识别的智能客服和语音助手，智能搜索、智能推荐等，可见目前的人工智能还是以特定应用领域为主的弱人工智能。不过，鉴于多数弱人工智能也拥有着收集信息能力、分析信息能力以及作出决策能力，它可以通过收集和分析数据来了解背景，对外部环境的变化做出反应并作出更智能的选择。

随着人工智能在创造其生成物时所占的贡献比例越来越大，如果相应知识产权保护的法律体系依然像保护传统计算机软件一样保护人工智能及其生成物，毫无疑问可能会造成相关主体对于法律的理解及适用的混乱。人工智能的发展亟需知识产权保护制度的更新。

3.参见吴汉东:《人工智能生成发明的专利法之问》,《当代法学》2019年第4期

PART 02
人工智能本身的可专利性

关于人工智能领域技术本身的可专利性问题，例如在开篇提及的小i机器人公司诉苹果公司的案件，关于小i机器人专利有效性问题一直讨论到8年以后才尘埃落定。《专利法》第二条对“可专利主体”有一个明确的定义，即“本法所称发明创造，是指发明、实用新型和外观设计。”发明是指关于产品、方法或者其改进的新的技术方案。实用新型是指由产品的形状、结构或组合提出的适合实际使用的新的技术方案。外观设计是指通过产品形态、图案或它们的组合，以及颜色、形状和图案的组合，使产品具有美感，适合工业应用的新设计。《专利法》第二十五条规定：“科学发现、智力活动的规则和方法等不得授予专利权。”而在人工智能领域，算法的创新是技术层面上每一项发明和创造的核心，纯粹的算法本身属于智能活动的规则和方法，笔者理解，根据《专利法》第二十五条，不能授予其本身专利权。

关于计算机程序的可专利问题。通常而言，计算机程序是算法的一种，本身属于智力活动的规则，不能授予专利权。修改后的《专利审查指南》对“计算机程序本身”与“涉及计算机程序的发明”做出严格区分，前者不属于“可专利主体”，但允许后者采用“介质+计算机程序流程”的方式撰写权利要求书，进而获得专利授权。[3]

不过目前在司法实践中，国家知识产权局专利复审委员会在作出决定时没有一套非常明确的标准，意味着在人工智能本身是否受到专利法的保护这一问题上，尚也存在着争议和可讨论空间。

PART 03

人工智能生成物能否受到法律保护？

1、能否受到《著作权法》的保护？

现阶段，人工智能生成物与人的创造物的差距正在快速缩小，有时几乎可以做到没有差别，他们能否构成《著作权法》下作品或者专利法保护的发明？《著作权法》第三条规定："本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果。"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。

针对独创性的界定，《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。"[4]因此，在判断该生成物是否具有独创性时，还应当结合个案具体分析。

随着大数据、神经网络等技术的发展，人工智能可以模拟人脑中神经元的深度学习，从庞大的数据库中自动选择所需的材料进行集成处理。人工智能的作用已经远远超过最初的辅助性工具定义，例如在新闻写作领域，人工智能系统腾讯写稿机器人Dreamwriter可以独立完成新闻写作，在财经、科技应用、体育赛事等领域撰稿戳过两千篇。[5]人工智能对创造的贡献越来越大，有时候，人工智能甚至可以独立完成整个创作过程，创作出可以被认为是"原创"的艺术、音乐和文学作品。此时，当人工智能不仅仅再局限于辅助工具，其生成物的表达体现了其特有的选择和判断时，笔者认为可以符合独创性要件。

但就我国现有的知识产权制度来说，目前人类的智力活动是专利和著作权保护的构成要素之一。在当前《著作权法》框架下，赋予人工智能本身人格权尚且不太可能，考虑到人工智能本身无法成为《著作权法》项下的适格作者，完全没有人类参与的人工智能自主生成产物，基于目前法律，尚无法被视为作品。在我国，北京互联网法院在全国首例人工智能生成内容著作权纠纷案【(2018)京0491 民初239号判决书】中裁定：自然人创作的作品完成仍应是中国版权法作品的必要条件。因此，计算机软件智能生成的案件相关分析报告不属于版权法意义上的作品，不包括人工智能作品的版权。

4. 陈际红 钱璐："人工智能生成物能否获得法律保护？"，http://www.zhonglun.com/Content/2020/03-10/1719302944.html，2020.03

5.刘鑫、覃楚翔："人工智能时代的专利法：问题、挑战与应对"，《电子知识产权》2021年第1期，第73-82页

6.最高院知识产权审判庭周波法官："人工智能与著作权保护——中国法院的司法实践"

7.刘强、张佳明："人工智能知识产权创作者资格问题研究"，《武陵学刊》2019年第4期，第45-52页

就目前的技术发展来说，人工智能尚未发展到完全脱离人类参与的水平。基于《著作权法》等法律规定，我们可以看出，保护著作权相关的立法目的在于加强创作者权益的保护，促进文学艺术的进步与创新，促进文化与科学事业的繁荣。由于人工智能已经在很多领域得到了广泛应用，对人工智能生成物的保护，我国司法实践也正在加紧探索，例如在Dreamwriter案中，法院经审理认为：Dreamwriter软件生成的涉案文章属于原告主持的多团队、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。因此是中国《著作权法》所保护的文字作品，原告对其享有著作权。[6]

2、能否受到《专利法》的保护？

根据我国的《专利法》，受《专利法》保护的发明均要满足新颖性、创造性和实用性的要求。《专利法》第二十二条第四款规定的"新颖性"要求："新颖性是指发明或者实用新型不属于现有技术;申请日前，任何单位或者个人未就同一发明或者实用新型向国务院专利行政部门提出申请，应当在申请日后公布的专利申请文件或者专利文件中予以记载。通过技术方案与"现有技术"的比较，具体操作方法是由技术人员在同一现场进行搜索，并对现有技术进行比较，判断两者的技术特点是否相同。如果人工智能发明足够新颖，就可以申请专利。"

但是，对于人工智能根据搜集到的信息形成的技术方案是否具有新颖性、创造性在实践中具有一定不确定性，缺少统一的判断标准，同时《专利法》还要判断人工智能创造物是否达到实用性标准，这也是对目前司法实践中的一种挑战。

PART 04
人工智能生成物权利主体认定

1、人工智能生成物的著作权主体争议

"青蛙儿正在远远的浅水，她嫁了人间许多的颜色"这句诗出自微软研发的人工智能产品——"小冰"之手。此前，"小冰"还创作并出版了诗集《阳光失了玻璃窗》。2017年7月5日，微软（亚洲）互联网研究院宣布放弃小冰所著诗歌版权，开启人工智能与人合著新模式。公告称，小冰会完成初步创作，人类在此基础上完成创作，并且人类能独享该诗歌最终作品的全部权利。[7]那么，微软研究院在宣布放弃微软小冰诗版权之前是否拥有该人工智能生成物的

版权呢?人工智能本身能否成为其生成物的著作权人呢?

首先,笔者认为应该给予人工智能本身一定的署名权,如果将署名权给予了人工智能的发明者或者使用者,实际上该发明者或者使用者对于该作品并无太大贡献,则与事实并不符合。但是笔者在此需要明确的是,给予署名权并不意味着承认人工智能的著作权主体地位。

2021年6月1日起生效的新《著作权法》的第十一条规定:“著作权属于作者,本法另有规定的除外。创作作品的自然人是作者。由法人或者非法人组织主持,代表法人或者非法人组织意志创作,并由法人或者非法人组织承担责任的作品,法人或者非法人组织视为作者。”从法条本身的描述可见,我国《著作权法》规定的著作权主体是自然人、法人或其他组织,现行法律尚未将人工智能纳入作者的范畴。假设法律赋予了人工智能著作权主体的地位,那么当侵权行为发生,就有可能会造成侵权责任主体不明的情况。如果人工智能在运行过程中侵犯他人权利,且人工智能本身被赋予了法律主体地位,那么就理应由实施了侵权行为的行为人(即人工智能本身)来承担相应的侵权责任。此种情况下,笔者认为极有可能致使人工智能使用者和发明者逃脱一定的责任。从这个角度上看,只有当人工智能生成物的著作权主体是自然人、法人或其他组织时,才能使法理有一个闭环。在前述Dreamwriter案中,法院就是判定Dreamwriter的作品是原告主持创作的法人作品,由原告对其享有著作权。

但是,人工智能生成物的作者是属于软件开发者还是实际用户?国际标准化组织(iso)也在其标准草案文件《道德设计:使用人工智能和自主系统(ai/as)实现人类福祉最大化的愿景》(*Ethical Design: a vision for maximum human well-being using artificial intelligence and autonomous systems*)中提出,“如果人工智能和自主系统依靠人类互动来创造新内容或发明,那么使用它的人应该是作者或发明者。”[8]从学理上看,这一说法也有一定道理。《著作权法》是为了保护并激发创作者创作的积极性,促进经济、科技的发展和文化、艺术的繁荣。人工智能的实际使用者使用人工智能进行创造,将人工智能生成物的作者和权利主体认定为实际使用者的制度是其创造的肯定。这样的保护又能激励人工智能使用人的创作热情,继续利用人工智能创作出新的作品,形成一个良性循环。

综上分析,在认定人工智能生成物的著作权归属时,笔者认为可以参考职务作品的保护方式对人工智能生产作品进行著作权保护:人工智能享有署名权,著作权的其他权利由人工智能使用人(类比雇员的法人或者非法人单位)享有。

8.朱琳:“浅论人工智能创作物的知识产权保护”,《法治追踪》2019年,第233-235页

2、人工智能生成物的专利权主体争议

9.35 U.S. Code § 116

10.Hess v. Advanced Cardiovascular Sys., 106 F.3d 976, 981 (Fed. Cir. 1997)

就现有的知识产权主体制度来说，目前人类的智力活动是专利和著作权保护的构成要素之一，想要将人工智能认定为其生成物的权利主体存在一定的制度障碍。以《专利法》为例，虽然《专利法》没有明文规定只保护人类智力的成果，但是我国专利申请实践中，专利请求书必须写明发明人的姓名，而其中发明人应是自然人，即便是可以独立享有民事权利和义务的法人也不能成为发明人。在美国，申请专利的规则更加严格，如果发明人没有被点名或者被错误申请，该专利就存在被宣布无效的风险。在该种情况下，人工智能能否对其生成物享有主体权利存在不小的争议。

美国涉及人工智能技术的专利诉讼中，有一个争议焦点就是对于发明人的认定，人工智能自身能否一并成为其发明创造的专利所有权人?美国法项下的答案是否定的。根据《美国法典》第35编专利编中第116（a）项[9]规定，“发明者”的意思是“发现或创造了发明对象的个人”，对共同开发者的描述是一同创造了发明的“两人”或“多人”。共同开发者不一定是发明人。在著名的Hess v. Advanced Cardiovascular Sys.一案中，法院认为：“一个发明者可以利用他人的服务、意见和帮助完善自己的发明而不至于失去他申请专利的权利”[10]，共同开发者为发明提供了建议和帮助，但这些贡献并不必然

构成共同发明人。联邦第二巡回法院在New Idea Farm Equip. Corp. v. Sperry Corp.一案中明确了某些法律实体不得取得发明者的身份，因为它应为“个人而非公司所开发的”。结合上述两起经典案例，在美国的诉讼实例中，法院并不承认人工智能对其发明创造的专利主体地位，而是将该主体地位赋予给了人工智能的发明者或者投资者。

正如上文所言，基于技术发展的限制，现有的人工智能在大多数情形中都还只能起到一种发明辅助作用。对于人工智能在《专利法》项下的权属认定，笔者认为也可参考上文人工智能生成物的著作权归属的方法，比照我国《专利法》中职务发明专利、雇佣发明专利的相关规定，赋予人工智能的创造人或者投资人以人工智能发明的专利权主体资格。

PART 05
人工智能带来的不正当竞争问题

人工智能的核心在于算法，基础在于数据，而算法的垄断和数据的保密会带来人工智能领域的限制竞争与垄断风险，会对市场的正常竞争秩序造成影响。人工智能的深度学习技术需要大量的数据，这就使数据具有非凡的经济价值。从竞争法的角度来看，利用算法和数据实施垄断行为可能阻止新型企业进入市场抢占市场份额，如何在人工智能知识产权与数据保护和防止数据垄断之间找到动态的平衡，也是当前国内外竞争法实践项下所共同面临的一大挑战。

2017年，中国修改了《反不正当竞争法》，增加了第十二条互联网条款，列举了“经营者不得以技术手段影响用户的选择或者其他方式实施下列妨碍或者干扰其他经营者合法提供的网络产品或者服务正常运行的行为：（一）未经其他经营者同意，在其合法提供的网络产品或者服务中，插入链接、强制进行目标跳转；（二）误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的网络产品或者服务；（三）恶意对其他经营者合法提供的网络产品或者服务实施不兼容。”除此之外，第四款中也做出了相应概括性规定，即“其他妨碍或者干扰其他经营者合法提供的网络产品或者服务正常运行的行为”。司法实践中，人工智能市场存在大量利用技术实施不正当竞争行为的现象，目前主要通过《反不正当竞争法》以及《反垄断法》的相关法规进行规制。

未来已来，人工智能已经悄然来到了我们的身边，契合人工智能的特点和发展方向，哪种知识产权保护方法更有利于促进产业的发展，如何厘清人

工智能知识产权的保护边界，是我国当前司法实践中亟需思考、探讨和解决的问题。

王红燕
合伙人
知识产权部
杭州办公室
+86 571 5662 3968
gracewang@zhonglun.com

人工智能创新的知识产权布局与保护

作者/张鹏

人工智能创新是提升国家竞争力的重要方面，利用知识产权制度激励人工智能创新创造、促进人工智能产业发展非常关键。人工智能的迅猛发展不仅仅是一个科学技术领域的新现象，它正在迅速改变人类社会的经济形态、社会交往模式和政治——法律结构[1]。

作为一项引领未来的战略性技术，世界主要国家都将人工智能创新作为提升国家竞争力的重要方面。美国早在2011年就出台了《国家机器人计划》，并于2017年出台了《国家机器人计划2.0》和《人工智能未来法案》，2019年出台了《国家人工智能研发战略规划2019年更新版》《人工智能倡议行政命令》等多项战略决策，从战略层面部署人工智能产业的创新创造。日本在2015年出台了《新机器人战略》，2017年出台了《人工智能技术战略》，2019年出台了《针对所有个体的人工智能战略：公众、产业及政府》，强化人工智能领域创新，并强调及时发现解决人工智能领域创新中的知识产权问题。欧盟2018年发布人工智能战略，制定欧盟人工智能行动计划，并于2020年发布《面向卓越和信任的欧洲人工智能发展之道》和《知识产权与人工智能》报告[2]。

顺应时代的发展和技术潮流，我国也相应做出了人工智能创新方面的战略部署，《国民经济和社会发展第十四个五年规划和2035年远景目标纲要》提出："聚焦……人工智能关键算法、传感器等关键领域，加快推进基础理论、基础算法、装备材料等研发突破与迭代应用。培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业。"同时，我国也高度注重利用知识产权制度激励人工智能创新创造、促进人工智能产业发展。国务院《新一代人工智能发展规划》明确要求"建立人工智能技术标准和知识产权体系"，专门部署"加强人工智能领域的知识产权保护，健全人工智能领域技术创新、专利保护与标准化互动支撑机制，促进人工支撑创新成果知识产权化。建立人工智能公共专利池，促进人工智能新技术利用与扩散"。工业和信息化部《促进新一代人工智能产业发展三年行动计划（2018-2020年）》专门强调，"支持建设专利协同运营平台和知识产权服务平台"。从处于人工智能产业这一典型的知识产权密集型产业的企业层面而言，迫切需要加强人工智能创新的知识产权布局与保护，尽早实现特定人工智能应用场景的"跑马圈地"，维护自身在人工智能产业的核心竞争力。

1.郑戈："人工智能与法律的未来"【J】，载于《探索与争鸣》2017年第10期。

2.王迁、陈树森、陈绍玲、刘鹏、袁锋："人工智能知识产权保护问题研究"【C】，载于崔亚东主编：《世界人工智能法治蓝皮书(2020)》，"第五部分人工智能法治发展专题报告"，第193-204页。

PART 01

人工智能创新的知识产权综合布局

3.袁曾：“人工智能有限法律人格审视”【J】，载于《东方法学》2017年第5期。

人工智能创新难以运用某一类型的知识产权进行保护，需要在现行法律制度框架下开展知识产权保护。由于现行法律体系对于人工智能的法律人格规制有缺位，造成实践应用缺乏法律价值指引，人工智能的法律地位和具体规制亟待明晰[3]。虽然如此，作为企业角度来说，我们不能等待人工智能法律制度的完善，而是需要在现行法框架下开展人工智能创新的知识产权保护。

人工智能创新的实现方案在著作权保护方面均存在一定空间，亦存在不足之处。就人工智能创新的实现方案而言，由于思想表达二分法下仅仅保护作品的表达，使得软件著作权对人工智能基础算法的保护非常有限。这也是20世纪后叶以来“软件专利”应运而生的重要原因。通常而言，包括人工智能基础算法在内的算法实现形成软件的过程在于，需求分析与架构设计、详细设计与编写代码、代码测试与软件发布三个环节。

第一是需求分析与架构设计环节。相关系统分析员向用户初步了解需求，然后用相关的工具软件列出要开发的系统的大功能模块，每个大功能模块有哪些小功能模块，对于有些需求比较明确相关的界面，在这一步里面可以初步定义好少量的界面；系统分析员深入了解和分析需求，根据自己的经验和需求用WORD或相关的工具再做出一份文档系统的功能需求文档。这次的文档会清楚列出系统大致的大功能模块，大功能模块有哪些小功能模块，并且还列出相关的界面和界面功能。开发者需要对软件系统进行架构设计，对软件系统的设计进行考虑，包括系统的基本处理流程、系统的组织结构、模块划分、功能分配、接口设计、运行设计、数据结构设计和出错处理设计等，为软件的详细设计提供基础。

第二是详细设计与编写代码环节。在架构设计的基础上，开发者需要进行软件系统的详细设计。在详细设计中，描述实现具体模块所涉及到的主要算法、数据结构、类的层次结构及调用关系，需要说明软件系统各个层次中的每一个程序(每个模块或子程序)的设计考虑，以便进行编码和测试。应当保证软件的需求完全分配给整个软件。详细设计应当足够详细，能够根据详细设计报告进行编码。在软件编码阶段，开发者根据《软件系统详细设计报告》中对数据结构、算法分析和模块实现等方面的设计要求，开始具体的编写程序工作，分别实现各模块的功能，从而实现对目标系统的功能、性能、接口、界面等方面的要求。

第三是代码测试与软件发布环节。测试同样是项目研发中一个相当重要的步骤，对于一个大型软件，3个月到1年的外部测试都是正常的，因为永远都会有不可预料的问题存在。完成测试后，完成验收并完成最后的一些帮助文档，整体项目才算告一段落。就这三个环节形成的智力活动的成果而言，第一个阶段形成的是软件架构，第二个阶段形成的是软件代码，第三个阶段形成的是测试报告。显然，软件著作权仅仅能够保护软件代码的表达，无法保护软件代码所体现出的“软件架构”。同时，随着软件产业的不断发展，尤其是自动编程工具和辅助编程工具的日益成熟，软件架构的创造性劳动价值更加凸显。

人工智能创新的实现方案在专利权保护方面存在一定空间，算法创新的专利权保护还需要制度规则的进一步完善。2019年12月31日，国家知识产权局发布《关于修改<专利审查指南>的公告（第343号公告）》，对“包括算法特征或者商业规则和方法特征的发明专利申请”的审查基准进一步调整，虽然并非专门针对人工智能技术，但是基于人工智能技术的核心在于算法，从而对人工智能技术相关专利申请的审查有较高的指导意义。此次修改内容已经于2020年2月1日开始实施。此次修改在现行《专利审查指南》第二部分第九章第1-5节之后增加了完整的第6节，专门针对“包含算法特征或商业规则和方法特征的发明专利申请审查”作出相关规定。对于人工智能技术这类包含算法特征或商业规则和方法特征的发明专利申请，需要从三个方面进行审查，同时这三个方面具有逻辑联系：首先，审查涉案专利申请是否属于专利法意义上的保护客体；其次，审查权利要求是否以说明书为依据，清楚、简要地限定要求专利保护的范围；最后，审查权利要求是否具有新颖性和创造性。由于我国对于人工智能技术这类包含算法特征或商业规则和方法特征的发明专利申请需要从三个方面进行审查，既要满足类似“拟制现有技术排除测试法”的要求，也要满足类似“技术属性测试法”的要求，由此导致我国人工智能技术专利申请的授权确权存在相当的难度。人工智能技术的核心在于基础层的基础算法，然而传统的专利法律制度认为算法属于智力活动的规则和方法，从而人工智能技术理应被排除在专利法的保护范围之外[4]。

此外，技术秘密保护以及反不正当竞争法的行为规制，对人工智能基础算法的保护亦有空间。

4.张洋：“论人工智能发明可专利性的法律标准”【J】，载于《法商研究》2020年第6期。

PART 02

人工智能技术的专利布局

人工智能技术通常分为基础层、感知层、认知层、应用层四个层次，需要实现立体式的专利布局。基础层是实现大计算驱动和大数据保障的基础算法，感知层主要体现为语音技术、图像技术、视频技术、AR/VR增强现实基础等感知性技术，认知层主要体现为人工智能涉及的自然语言处理、知识图谱、用户画像等以机器学习为核心的认知性技术，应用层主要是无人驾驶、智能制造等应用场景。截至2020年底，中国人工智能相关企业数量达到6425家；其中，22.3%的企业分布在人工智能产业链的基础层，18.6%的企业分布在人工智能产业链的感知层、认知层，59.1%的企业分布在人工智能产业链的应用层。

我国国家工业信息安全发展研究中心、工业和信息化部电子知识产权中心发布的《2020人工智能中国专利技术分析报告》表明，截至2020年10月，中国人工智能专利申请量累计已达69.4万余件，同比增长56.3%，中国人工智能技术专利申请总量首次超过美国，成为全球申请数量最多的国家。中国人工智能专利技术分支统计显示，云计算作为人工智能的基础支撑技术，专利占比最多，达到18.38%；计算机视觉作为人工智能领域的应用技术，紧随其后，占比为17.72%。深度学习、自动驾驶及智能机器人各占比为14.52%、12.36%和9.55%。其后按照占比数值排序分别是占比7.58%的交通大数据、占比5.72%的智能推荐、占比5.65%的自然语言处理、占比5.35%的智能语音、占比3.16%的知识图谱技术。

人工智能技术的立体式专利布局可以借鉴药品的“化合物专利——组合物专利——制备方法专利——变换性专利——用途专利”的立体式专利布局模式[5]。

5.邱福恩：“人工智能算法创新可专利性问题探讨”[J]，载于《电子科学技术》2020年第1期。

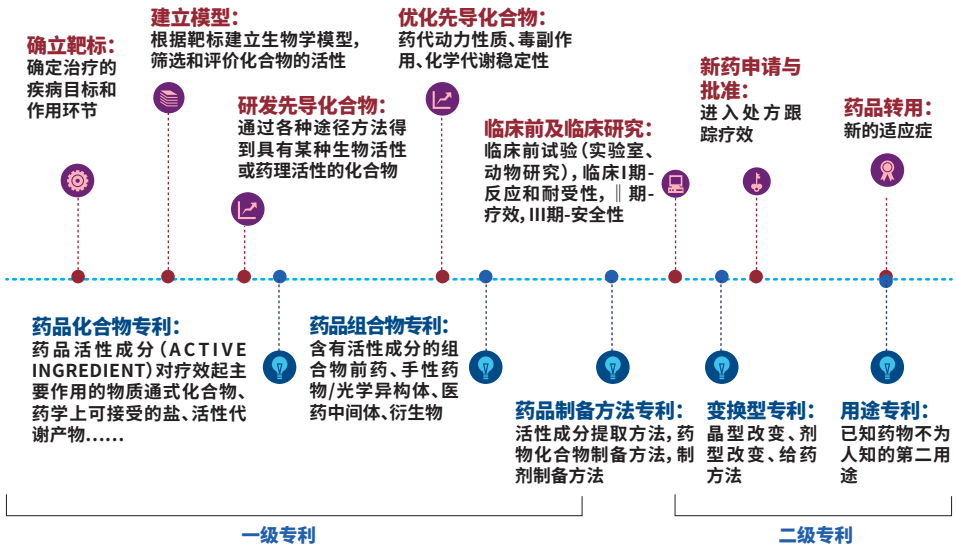


图1 可以作为参照的药品专利立体布局模式

如图1上半侧所示，药品研发过程（或者称为药品创新链）通常包括确立靶标、建立生物学模型、研发先导化合物、优化先导化合物、临床前及临床研究、新药申请与批准、药品转用等环节。其中，确立靶标、建立模型、研发先导化合物、优化先导化合物这四个步骤，通常被认为是药品的研究阶段；临床前及临床研究、新药申请与批准、药品转用这三个步骤，通常被认为是药品的开发阶段；药品的研究阶段和开发阶段统称为“药品的研发过程”或者“药品创新链”。在药品创新链中，“确立靶标”是创制新药的出发点，用以确定所需要治疗的疾病目标和作用的环节。在确定了靶标之后，通过建立生物学模型的方式筛选和评价化合物的活性，通常来说需要建立药代动力模型。在确立靶标、建立模型之后，研发先导化合物[6]。在药品创新链中，在进行药品研究后进行临床前及临床研究、新药申请与批准、药品转用这三个药品开发步骤。

临床前研究主要是，对药品进行实验室或者动物研究，确定药物活性和安全性。与上述药品创新链相适应，药品专利布局链通常为，在确立靶标、建立生物学模型之后，(1) 为了确定先导化合物通常需要对相关领域的专利进行检索，形成先导化合物需要形成先导化合物专利。先导化合物专利对通式化合物、药学上可接受的盐、活性代谢产物进行专利保护。先导化合物专利基本上是一款药品最为基础的专利。同时，因为先导化合物专利化学结构相同的药物，可因结晶条件不同而得到不同晶体，药物多晶型现象也是影响药品质量与临床药效的重要因素之一。需要强调的是，药物科学是一门试验学科，化学结构相同的药物，可因结晶条件不同而得到不同晶体，药物多晶型现象也是影响药品质量与临床药效的重要因素之一。例如，目前畅销的抗血

6. 所谓“先导化合物”，是指通过各种途径和手段得到的具有某种生物活性和化学结构的化合物，这对于药品研究而言非常重要。先导化合物主要有如下几个来源：对天然活性物质的挖掘、现有药物不良作用的改进以及药物合成中间体的筛选等。由于先导化合物可能具有作用强度或特异性不高、药代动力性质不适宜、毒副作用较强或是化学或代谢上不稳定等缺陷，一般不能直接成为药物。因此，在研发先导化合物之后根据药代动力性质、毒副作用、化学代谢稳定性等对该先导化合物进一步优化。

栓药硫酸氢氯吡格雷，其左旋异构体在50 mg/kg 的给药剂量时会产生明显的神经毒性，但是右旋异构体无神经毒性，因此上市的是右旋异构体。因此，在优化先导化合物的过程中，形成组合物专利，通常是就两种或两种以上元素或化合物按一定比例组成具有一定性质和用途的混合物的技术方案申请形成的专利。[7]这就是上述所言，在化合物专利基础上配合组合物专利进一步加强专利布局。

在此之后，(2) 进一步形成药品制备方法专利，包括组合物的提取分离方法、提纯方法、制备方法等。由于化合物专利、组合物专利、药品制备方法专利形成于药品研究阶段，创新程度较高，通常被认为是药品一级专利或者药品一类专利。(3) 在临床前及临床研究、新药申请与批准阶段，通常会产生药品的变换型专利，例如晶型等。(4) 在药品转用阶段产生用途专利，如化学物质的新的医药用途、药物的新的适应症等。通常而言，变换型专利、用途专利被称为药品二级专利或者药品二类专利。虽然二级专利是依托于一级专利基础上的再创新，但是这并不意味着二级专利创新程度一定会比较低。这样的权利要求就属于《专利审查指南》第二部分第十章第4.5节规定的“用途权利要求”，亦即将基于发现产品新的性能，并利用此性能而作出的发明。[8]

同理，将研发过程与专利保护相嵌的方法也可适用于人工智能技术领域的专利布局（如图2）。建构“基础算法专利——感知技术专利——认知技术专利——应用场景专利”共同构成的人工智能技术专利布局。

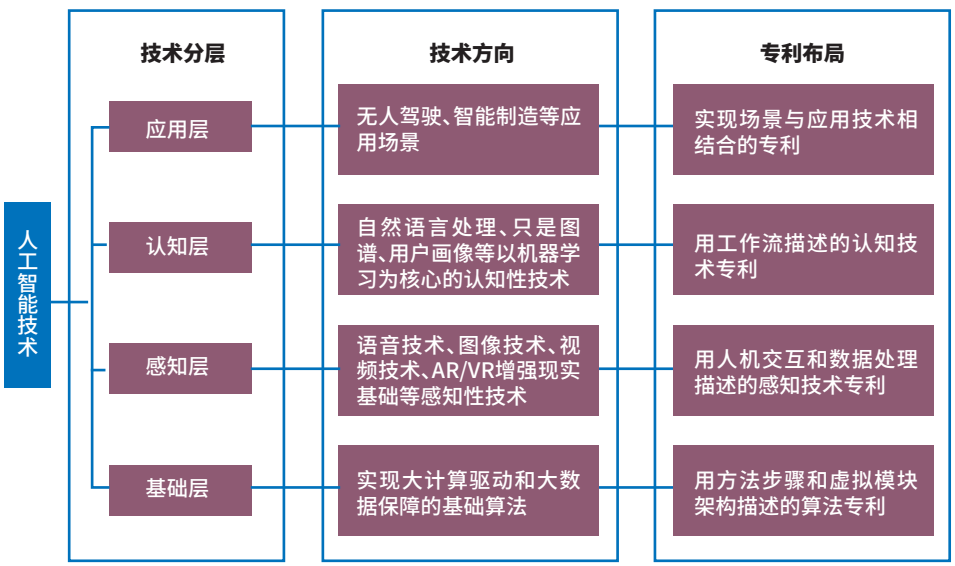


图2 人工智能技术立体专利布局模式

7.例如，辉瑞公司针对降血脂药阿托伐他汀于1986 年5 月30 日申请美国专利US4681893，保护含有阿托伐他汀的通式化合物及其药学上可接受的内酯水解盐，之后申请的后续专利US5273995 保护阿托伐他汀及其钙盐（即阿托伐他汀钙）。

8.详细讨论参见张鹏：“抗击疫情药物的用途专利申请前景与合规使用探析——以瑞德西韦专利布局分析为视角”【J】，载于《中国发明与专利》2020年第2期。

如前所述，人工智能技术通常包括基础层、感知层、认知层、应用层四个层次，基础层是实现大计算驱动和大数据保障的基础算法，感知层主要体现为语音技术、图像技术、视频技术、AR/VR增强现实基础等感知性技术，认知层主要体现为人工智能涉及的自然语言处理、知识图谱、用户画像等以机器学习为核心的认知性技术，应用层主要是无人驾驶、智能制造等应用场景。这其中，基础算法构成的基础层是整个人工智能技术的基础和核心，然而传统的专利法律制度认为算法属于智力活动的规则和方法，从而人工智能技术理应被排除在专利法的保护范围之外[9]。算法的专利保护，无非是在现有专利授权确权标准之下，根据促进人工智能发展的需求，划分出具有可专利性、可以授予专利权的“技术方案”和不具有可专利性、不能授予专利权的“智力活动的规则”[10]。

因此，需要通过撰写加工等方式，促进基础算法专利与应用场景或者感知技术、认知技术的结合，形成对基础算法的专利布局。特别需要注意的是，在寻求基础算法的专利保护过程中，需要与应用场景相结合时，必须认真分析基础算法除了当前应用场景之外的其他可能应用场景，对“场景替换式”的侵权行为进行有效规制。感知层主要体现为语音技术、图像技术、视频技术、AR/VR增强现实基础等感知性技术，可以采用人机交互和数据处理的方式加以描述，从数据流流向的角度总结处理流程形成方法权利要求，从模块架构出发形成装置权利要求。认知层主要体现为人工智能涉及的自然语言处理、知识图谱、用户画像等以机器学习为核心的认知性技术，可以采用工作流的方式从工作流流向的角度总结处理流程形成方法权利要求，从模块架构出发形成与方法权利要求对应的装置权利要求。应用层主要是无人驾驶、智能制造等应用场景，类似于上述药品专利的用途权利要求，将特定基础算法、特定感知层和认知层的工作流、数据流处理方案与应用场景进行结合，对特定应用场景下的使用进行保护。

9.张洋：“论人工智能发明可专利性的法律标准”【J】，载于《法商研究》2020年第6期。

10.孔祥俊：“人工智能知识产权保护的若干问题”【J】，载于《上海法学研究（集刊）（2019年第13卷 总第13卷）——上海市法学会互联网司法研究小组论文集》。

结语

根据《2021人工智能发展白皮书》的统计，2020年，中国人工智能核心产业规模达到3251亿元，同比增长16.7%；人工智能领域融资金额为896.2亿元，融资数量有467笔，人工智能领域单笔融资额达到1.9亿元，同比增长56.3%。对于目前正处于快速上升期、且以算法等技术作为企业核心竞争力的人工智能领域而言，相关企业必须紧跟技术发展热点和动态，根据不同业务的应用场景，将知识产权保护纳入人工智能创新的战略布局。

张鹏
合伙人
知识产权部
北京办公室
+86 10 5957 2068
zhangpeng@zhonglun.com

CHAPTER

2

人工智能的隐私保护挑战与应对

PRIVACY PROTECTION
CHALLENGE AND
COUNTERMEASURES
IN ARTIFICIAL INTELLIGENCE

观察•人工智能引发的隐私与数据保护风险

作者/周洋、徐颖蕾

1.人工智能概念(12):人工智能(一) https://mp.weixin.qq.com/s/4pPJDjAnwreBAcHed2Bgmg

PART 01
背景

人工智能("Artificial Intelligence"或"AI")是关于如何让机器实现人类智能的计算机科学。[1]人工智能在生产、生活中的应用已十分广泛,如无人工厂、智慧出行、自动驾驶等。人工智能表现出的超级算力已叹为观止,如2016年谷歌的AlphaGo连胜韩国围棋棋手李世石。人类在惊叹人工智能超级能力和效率的同时也面临人工智能对传统社会分工、法律关系乃至伦理带来的冲击。例如,2016年谷歌无人驾驶汽车在美国加州发生严重车祸,2020年疫情期间日本的人形机器人产品"陪伴机器人"受到追捧,2021年6月15日清华大学计算机系主创的虚拟学生"华智冰"正式入学等现象。只有了解人工智能的安全风险、隐私风险和伦理风险,对人工智能保持敬畏之心,才能科学地发展和利用人工智能。

目前,我国已开启有关人工智能的立法进程,敦促和规范人工智能发展。2017年国务院印发的《新一代人工智能发展规划》提出,我国人工智能发展的战略目标分三步走。具体而言,第一步即到2020年"部分领域的人工智能伦理规范和政策法规初步建立";第二步即到2025年"初步建立人工智能法律法规、伦理规范和政策体系,形成人工智能安全评估和管控能力";第三步即到2030年"建成更加完善的人工智能法律法规、伦理规范和政策体系"。针对人工智能伦理,我国也出台了《网络安全标准实践指南—人工智能伦理安全风险防范指引》,为组织或个人开展人工智能研究开发、设计制造、部署应用等相关活动提供指引。在未来,对于人工智能的立法将会更加丰富,我国将会建立起更加全方位、多主体的人工智能法律体系。本篇主要从人工智能引发的隐私风险和数据保护风险角度对人工智能的发展作出冷思考。

PART 02
人工智能引发的隐私风险

人工智能的技术核心主要包括数据和算法,这意味着人工智能水平越高,越需要大数据喂养,还需要算法不断练习。这些数据很可能包含大量个人信息,而个人信息中的隐私信息一旦泄露,则会造成难以估量的后果。具体而言,人工智能技术引发的隐私风险体现在以下几个方面:

1. 人工智能使私密空间处于监控之下

人工智能技术的入侵会模糊私密空间的边界，使原本私密的空间处于监控之下。人工智能的应用场景决定了它本身需要获取大量的隐私信息。各种人工智能产品，小到可穿戴的智能设备（如智能手环），大到无人驾驶汽车，其装载的摄像装置、传感装置、语音录取装置等，都需要进入个人的私密空间甚至人体，才能收集、记录个人的行为、表征、轨迹、偏好并通过运算发出指令。因此，在多数场景下人工智能天然与隐私密不可分。

例如，自动驾驶场景下，车辆不仅要收集车外数据还需要收集车内数据，包括驾驶者的生理信息、语音和视频。而车内通常是个人的私密空间，人工智能将原本私密的空间变为数据收集场所，导致个人长期处于监控之下。如果被不当使用，人工智能设备将成为强大的窥探隐私的工具。

2.人工智能设备成为“隐私设置”的载体

有些人工智能设备本身就包含了隐私设置。例如，未来可能将在人们的生活中扮演重要角色的社交型机器人，它们为个人提供陪伴、聊天、学习以及看护等服务。为了使社交型机器人更了解用户从而实现高度智能的交互功能，用户需要对其完成初始“隐私设置(setting privacy)”，包括输入生理信息、行为偏好、兴趣偏好等各种隐私信息。不仅如此，随着与社交型机器人交互的不断深入，个人将逐渐展现其最为私密的心理属性(psychological attributes)。而社交型机器人则在用户不设防的状态下通过持续的信息收集和深度学习掌握到用户最私密的信息。用户在使用包含隐私设置的AI设备时，需要注意数据保护风险。

3.人工智能使用户“画像”更为容易

人工智能中的算法经常被用于用户画像，通过算法对人的隐私作出分析和预测。通过Cookie、Fingerprinting[2]等技术，可以实现个人信息的识别、追踪与收集。在商业领域，越来越多的企业开始收集个人的浏览记录、购买记录、交易方式等信息，依据这些信息来分析用户行为，对网络用户进行用户画像和精准营销。例如在新闻资讯与娱乐领域，抖音、快手、今日头条等利用算法进行个性化推荐与分发，以提高新闻与娱乐资讯的传播效率；在电商领域，淘宝、京东等购物网站利用算法对个体进行个性化商品推荐，以大幅促进销量。但同时，人工智能也成为实施“大数据杀熟”和“歧视性定价”的工具。

2.”Fingerprinting”技术通过交叉比对关键信息验证来识别计算机。就像在现实社会中人们可以通过指纹来识别特殊的个体一样，服务器在传输过程中可以利用传输的关键信息来识别某台计算机。例如某个网站可以识别用户使用的浏览器类型，用户使用的字体，以及网站在计算机上安装的插件。这些信息可能都不是唯一的，但是结合起来，它们可以识别唯一的个体。

4.人工智能造成“信息茧房”(信息牢笼)

2006年哈佛大学凯斯•桑斯坦在他的《信息乌托邦》中提出了“信息茧房”概念。桑斯坦指出,在信息传播中,公众所接触的信息是有限的,会选择自己愉悦的信息,久而久之,会将自身桎梏于像蚕茧一般的“茧房”中,失去思考的能力。个性化推荐本质上并不是用户在主动选择信息,而是将信息主动推送给用户。用户所接触到的信息要么是夺人眼球的“10万+”,要么局限在他们感兴趣的狭小领域,要么就是与他们观点和意见相一致的“溺爱式”信息。在很大程度上,用户被算法所提供的信息“喂养”,沉浸在算法制造的信息茧房/牢笼里,久而久之丧失独立思考能力。

不仅如此,基于算法的精准推送还剥夺了用户不被打扰的权利,即隐私的权利。美国隐私权先驱萨缪尔•沃(Samuel War-ren)和路易斯•布兰迪斯(Louis Brandeis)就在其名作《隐私权》一文中提出,隐私权是人们享受独处的权利(right to be alone)。笔者理解在一定程度上,精准推送剥夺了用户选择信息和不被打扰的权利,是一种新型的侵犯隐私方式。

PART 03

人工智能技术引发的数据保护风险

从数据保护角度来看,人工智能是一种数据处理活动。人工智能算法尤其是在深度学习过程中,需要大量数据样本和算法练习。但如果数据被污染、泄露、滥用,则不仅会影响输出结果,还可能危及人身财产安全、社会经济秩序甚至国家安全。因此,在人工智能数据的收集、存储、使用、分享、传输、销毁方面都需要有法可依,有章可循。

1.“数据污染”影响人工智能决策的准确性

人工智能需要处理大量数据,因此数据质量直接决定了人工智能的效率。数据质量低下表现为“数据污染”和“数据偏差”。数据污染是指数据与人工智能算法不适配,从而导致算法模型训练成本增加甚至失效,本质是数据质量治理问题。数据偏差是指人工智能算法决策中所使用的训练数据,因地域数字化发展不平衡或社会价值的倾向偏见,使得数据所承载的信息带有难以用技术手段消除的偏差,从而导致人工智能的决策结果带有歧视性。例如,在金融征信、医疗教育和在线招聘领域,可能会因边远地区、弱势群体和少数族裔的数据量不足、数据质量不高等原因,导致自动化决策的准确率会基于人群特征形成明显的分化,从而产生实质性的歧视影响。此外,若污染

人工智能算法尤其是在深度学习过程中，需要大量数据样本和算法练习。但如果数据被污染、泄露、滥用，则不仅会影响输出结果，还可能危及人身财产安全、社会经济秩序甚至国家安全。因此，在人工智能数据的收集、存储、使用、分享、传输、销毁方面都需要有法可依，有章可循。

数据被用于政党竞选和政治宣传，则可能对政治生活产生极大冲击。

2. “数据投毒”带来人工智能决策的攻击性

除了客观原因，数据质量也可能因恶意干预而出问题。“数据投毒”是指人为在数据中添加异常数据或篡改数据，通过破坏原有训练数据导致模型输出错误结果，从而引发人工智能的决策偏差或错误，最终产生恶意攻击者所期待的结果。在自动驾驶、智能工厂等对实时性要求极高的人工智能场景中，数据投毒对人工智能核心模块产生的定向干扰将会直接扩散到智能设备终端（如智能驾驶汽车的刹车装置、智能工厂的温度分析装置等），从而产生攻击人身、财产的可怕后果。

3. 人工智能引发的数据争夺导致数据壁垒

由于人工智能的发展依靠大量数据的喂养，企业纷纷展开数据争抢。对于底层数据资源的竞争是人工智能企业最关键的市场竞争力体现。在这种情况下，企业、机构间不愿意共享、流通数据，而导致形成“信息壁垒”。而信息壁垒一定程度上阻碍了那些迫切需要大量数据来提升AI技术、增进人民福祉的企业或机构的发展。以医疗数据为例，医疗行业的数据对于提高诊疗效率、优化诊疗方案、促进临床试验等有举足轻重的地位，因而成为医院、药品企业、药械企业争抢的对象。政府与企业之间、大企业与小企业之间、行业与行业之间，因数据确权、数据安全等问题存在着诸多法律和技术上的数据壁垒，形成了“数据孤岛”。不仅极大制约了人工智能的发展，也成为滋生数据黑产的主要经济动因。成熟的医疗数据要素市场尚未形成，数据合法、便捷、安全、低成本的交易流通机制仍是空白，这远远无法满足医疗行业对于数据资源的需求，因此部分企业只能铤而走险，违规购买或违规收集数据。可见，一方面AI需要大数据支撑，另一方面也会带来数据争夺。因此，AI的发展需要安全、有序的数据分享机制，否则反而会阻碍数据流动形成数据孤岛。

4. 无差别数据收集可能危害国家安全

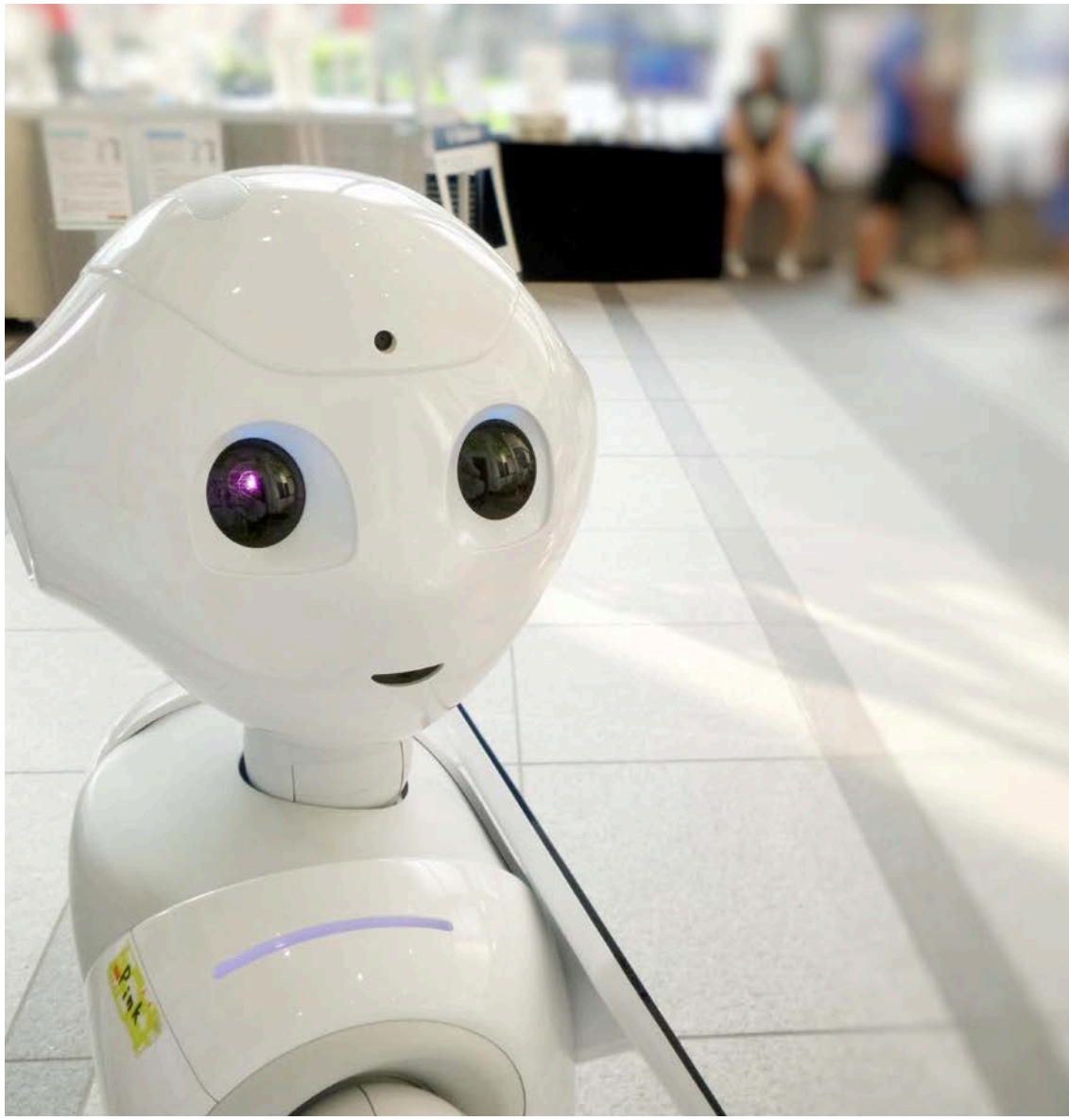
在人工智能技术研发和场景应用中均需要常态化、持续性、高速率、低延时的跨境数据流动。现场无差别收集是人工智能数据采集的重要方式，广泛应用于无人驾驶、智能家居、智慧城市等场景中。其主要通过在公开环境中部署各类传感器或采集终端，以环境信息为对象进行无差别、不定向的现场实时采集。

比如在智能网联汽车的无人驾驶场景中，自动驾驶汽车的传感器需要采集街景数据来支持智能驾驶系统的决策从而控制汽车行驶。但是这种无差别的街景数据采集必然会采集到行人的个人数据，甚至可能会采集到路边的重要基础设施分布、军事营区等重要数据从而给国家安全带来风险。而且在智能网联汽车领域，智能汽车产生的路况、地图、车主信息等大量数据可能回传至汽车制造商的境外服务器，进行产品优化升级和售后服务支撑。如果没有经过数据出境安全评估或网络安全审查，则可能带来个人敏感数据和重要数据出境后的安全风险。这种人工智能应用引发的跨境数据流动，不仅因各国日益趋严的数据安全规制和本地化要求而面临极大的法律障碍，更可能对国家安全、数据主权带来挑战。

总结

在人工智能技术高速发展的当下，我们既要看到其对生产、生活带来的有利影响，也要注意到其带来的隐私与数据风险。归根结底，此类风险的大小取决于人工智能的技术能力、使用意图和价值取向。因此，有必要通过立法规制人工智能的发展，提高人工智能的安全性，增强技术自身的“免疫功能”。同时也要对人工智能进行安全、伦理上的限制，建立起全方位的、由政府、企业、个人多方参与的人工智能法律体系。人类需要认识到，不了解人工智能风险就不能真正了解人工智能。

周洋
合伙人
知识产权部
上海办公室
+86 21 6061 3658
zhouyang@zhonglun.com



人工智能数据风险与治理

作者/陈际红、蔡鹏、焦雅婷

数据，是新时代企业发展的石油，对于人工智能行业发展而言更发挥着基础资源及助推器作用。人工智能在深度学习和机器学习领域的突破高度，有赖于高密度、高质量、多种类的数据支撑，其中不乏大量个人信息及非个人信息的收集处理，贯穿海量原始数据收集、内部存储管理、数据集运用（训练及测试）、第三方交互（功能支撑及技术运维等目的）、前端系统实际输出数据等各个阶段。可以说，人工智能的研发及运用周期，同时也是数据全生命管理周期。

围绕人工智能领域数据全生命周期管理，需重点关注如下风险：

PART 01
数据收集

在原始数据收集阶段，人工智能系统以模型训练、结果推断预测及输出等目的，通过用户主动提供、自动采集、间接获取等方式收集大量训练和应用数据集。保障数据可用性、可访问性、规范性、兼容性、机密性、关联性等，是决定人工智能技术有效性的重要环节。在本阶段常见风险情形包括：

一是是否充分遵循用户授权范围收集数据。在直接收集情形（多发生于现场数据采集场景）下，为满足多样化的应用需求，人工智能系统实际所收集的用户个人信息范围，存在超出用户授权同意的范围的情形。例如语音和语义识别，在收集必要的语音数据、设备信息的同时，可能基于个性化推荐等进一步需要，而附加收集地理位置等数据，但后者收集可能未囊括在前端隐私政策披露范围内。在间接收集的情形（例如网上爬取、外部数据源采购等，多发生于训练、测试数据采集场景）下，将用户数据等用于商业目的而非科研目的，可能面临数据收集处理与用户授权范围不相一致的合规风险。

二是是否合规收集生物识别信息。在人脸识别、语音及语义识别应用场景下，通常需要以用户面部识别数据、声纹数据等生物识别信息作为基础的数据源。目前国内外对于生物识别信息的监管日趋严格，以国内为例，新版《信息安全技术 个人信息安全规范》对于生物识别信息的收集及后续的存储管理均有明确要求，在明确告知用户且获取其明示同意的前提下，建议仅在前端收集并使用数据，后端存储尽量仅保留数据概要或者经匿名化处理的数据。与此同时，《信息技术 安全技术 生物特征识别信息的保护要求（征求意见稿）》以专门标准形式，讨论规制生物识别信息的收集处理问题。整体而言，对待以生物识别信息为代表的个人敏感信息的收集处理，需保持高度的

审慎性。

三是是否遵循最小必要原则，过度（过量或者过频）采集数据。鉴于人工智能模型训练需建立在高数量、多种类的数据的基础上，需关注所收集的数据是否均为实现该项目的所必要的，如何确保数据收集遵循必要原则、针对使用目的明确数据收集范围，属于实践中应当高度关注的合规要点。如涉及对用户个人信息的直接收集，需进一步关注收集量及频率的情况。例如，智能家居产品的应用，在方便用户日常生活的同时，也在全方位、随时随地、在用户毫无感知情况下获取和分析用户的浏览、位置、行程、沟通、搜索等信息，无止境的数据收集，也蕴含着更大的数据应用合规压力及应对泄露、非法使用的潜在风险。

四是如何保障数据收集质量。训练数据集的质量将对人工智能系统的可靠性和安全性起到至关重要的作用，而训练数据集规模不足、数据集的多样性和均衡性不足、数据集的标注质量低、数据集遭投毒攻击、数据噪声等问题，均将明显影响训练数据的质量。而对于现场数据而言，现场数据质量也将直接影响算法决策的输出，从而影响前端反应。

PART 02
数据存储

对于人工智能系统收集或产生的数据，通常存储地点分为本地现场存储（前端）、后端数据存储（数仓、底层数据池等）、云端数据库等存储系统，根据不同应用场景需求设计数据存储策略。例如，在智能安防、自动驾驶场景下，需要现场对数据进行实时分析、备份、回传、处理等；在智能家居、语义识别设备场景下，常见为云端处理及存储。数据存储媒介安全问题，包括系统安全漏洞、模型存储文件被破坏等，均可能造成数据泄露。对于人工智能系统所依托的智能硬件、软件环境，需高度重视信息安全设施建设及保障问题。

对于数据存储本身的合规风险，主要包括：在存储期限方面，是否在满足法律法规要求的最低存储期限的基础上，按照数据存储时间最小化的原则要求，结合业务及技术需要，合理制定数据存储期限，避免数据永久存储带来的合规风险；在存储措施方面，是否做到采取业内良好的技术保障措施，包括加密存储、物理分隔存储、访问权限管控等，以及针对生物识别信息采取匿名化处理、及时删除等存储。

PART 03
数据使用

在内部数据使用（数据分析和处理）阶段，涉及模型训练和部署运行过程，包括数据准备、数据挖掘、模型训练、测试验证、模型参数部署、预测结果输出等。其中数据准备主要对采集的原始数据进行预处理和标注等操作，以产生用于训练的数据集。在本阶段常见风险情形包括：

一是如何处理数据内部处理安全隐患及合规问题。受限于数据处理成本，大多数公司委托数据处理外包公司和自主处理相结合的方式进行数据处理，包括数据标注、数据挖掘、模型训练、数据清洗及筛选等工作。由于数据处理人员能够直接接触原始数据，如果内部数据安全管理制度体系不甚规范，可能存在数据窃取、未授权访问数据、数据投毒（以添加伪装数据或者恶意样本等方式破坏训练模型）、数据污染、泄露及非法利用数据等风险。随着人工智能与实体经济的深度融合，上述风险将可能进一步演化为对前端产业的影响。例如，在金融产品定价方面，数据投毒将导致定价结果不合理及投放选择不正确，进而影响金融企业的商业战略落实及部分金融消费者的权益实现。

二是如何合理应对自动化决策产生的结果导向及用户影响问题。利用个人信息训练的人工智能系统，通常需要考虑自动化决策的合规问题，即如何合理设置模型筛选、识别后的结果的自动运用，以避免其对用户合法权益的直接影响。例如，若金融行业采用人工智能算法（如在保险产品定价中应用AI模型算法），通过综合识别特定自然人的信用信息、交易信息等，自动筛选出特定金融产品的投放范围，则需在保障训练算法及模型的保密性的基础上，高度重视自动化决策机制设置的合理性、规则的透明性及可解释性，以及获取用户对筛选机制的同意，并保障数据主体的相应权利，避免对金融消费者的知情权、自主选择权等合法权益造成影响。

三是如何应对经去标识化处理后的数据的重识别问题。在数据准备阶段，通常使用数据预处理技术来提升数据质量，包括将外部获取的数据与内部已经完成去标识化处理的数据进行合并分析等。通过公开合法的手段收集分散的、无意义的数据点，组合形成扩展数据集，以综合推测出个人敏感信息（例如利用用户网上浏览痕迹来识别个人偏好及行为特征），可能导致已经被去标识化处理的数据可再次识别出特定自然人。

PART 04
数据共享

在数据传输方面，人工智能系统通常会根据实际需要，将主要功能组件分布于云端、本地服务器上，根据需要实现同步、异步数据备份及共享，在较短时间或者特定集中时间段内发生高密度的数据交互场景。例如自动驾驶场景内，支撑车联网及智能网联汽车的正常运行的数据，源自传感器、激光雷达等传感设备所采集的数据，其需通过车内网络进行快速、精准的数据传输。对于数据传输建立必要的安全保障措施，确保数据传输安全，降低数据泄露风险，属于人工智能系统建设时必须考量的要点。

在数据分享方面，基于部分功能场景支持及技术运维的目的，例如数据收集、数据标注、数据清洗、建模分析及数据测试、算法或者模型训练等，目前可常见部分人工智能公司会采取全部或部分委托第三方公司的方式进行，其间部分数据链路中所涉及的多方主体的数据保护能力参差不齐，可能带来数据泄露和滥用的隐患。如何保证数据在流通及共享过程中的安全使用、安全存储、安全销毁，对于人工智能服务企业而言为一大挑战。

而在数据跨境方面，以自动驾驶场景为例，鉴于目前部分技术服务分析商、图商、知名车企总部等位于境外，在境内采集获取的车辆数据、驾驶员操作数据、道路数据、驾驶街景数据、路径数据乃至气象数据等，都有可能共享至境外主体。其中可能涉及的个人信息、重要数据、特定领域（如气象数据、测绘数据等）的跨境传输的合规问题，包括是否额外提示用户、信息披露尺度、是否需额外申报或者备案、是否需进行出境合规评估等等，需引起人工智能服务企业的高度重视。

PART 05
数据合规案例分析与启示

（一）“美国威斯康星州诉卢米斯”案使用COMPAS算法量刑引争议[1]

1.案件事实

2013年2月，埃里克•卢米斯（Eric Loomis）被美国威斯康星州指控，在拉克罗斯市发生的枪击案中驾驶车辆，触犯了五项罪名。卢米斯对其中两项较轻的罪名，偷盗汽车和拒捕，表示认罪并请求法官判处缓刑。案件法官对卢米斯判处了六年监禁，裁判依据不仅仅是卢米斯的犯罪记录，还有COMPAS

1.https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/

系统中卢米斯对137个问题[2]的回答的算法结果。

COMPAS系统是Northpointe公司设计的一款风险需求评估工具，该工具最初被设计用于在收监、管理囚犯和规划惩治手段的过程中为监狱管理部门提供决策支持。目前，COMPAS系统已广泛应用在美国刑事诉讼程序中，其通过预测对象的再犯率、出庭可能性等因素，对其保释、量刑和假释做出决策，帮助法官做出“更好的”或者至少是以数据为中心的司法决策。

由于COMPAS系统的算法评估过程构成商业秘密，该公司不对评估因素的权重进行披露，卢米斯对量刑结果提出异议，认为其应有权知道被控告的理由，使用COMPAS系统进行风险评估侵犯了自己依据宪法享有的正当程序权利。

2.裁判结果

初审法院驳回了卢米斯的动议，且威斯康星州上诉法院和最高法院均在之后的判决中支持了下级法院的裁决。法院认为，被告的风险评估是基于他对137个问题的答案以及其犯罪历史等公开数据作出，且评估报告并不是法院裁决的唯一依据，法院有其自由裁量权，在适当时对报告提出异议或作出个体化裁决。此外，卢米斯还提出异议称，初审法院在判决时违宪地将性别纳入考量因素。法院针对这一点解释为，在风险评估中使用性别因素有助于提高准确性，而非出于歧视，且卢米斯并没有提供COMPAS系统的评估过程中使用了性别因素的证据[3]。

3.风险分析

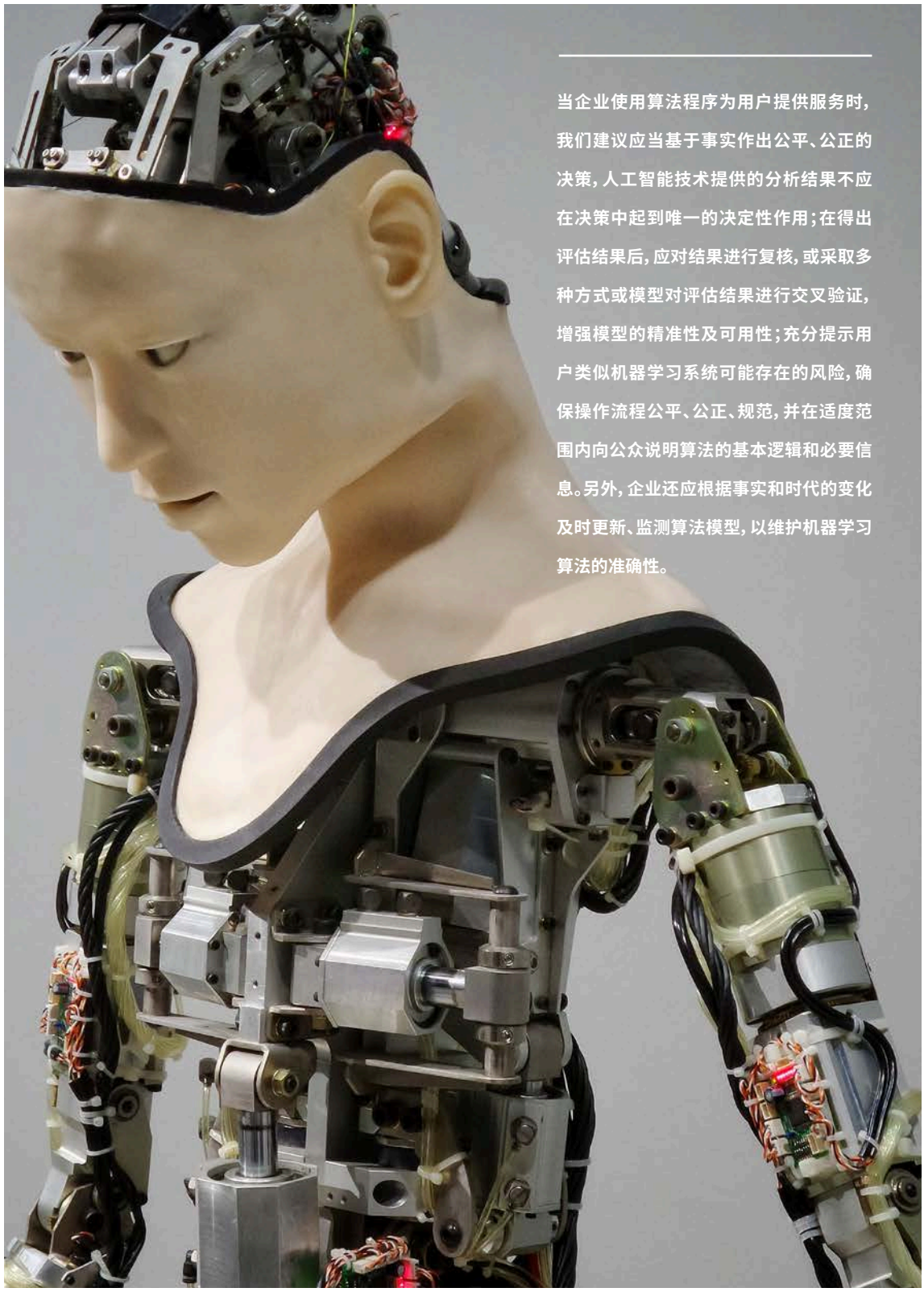
虽然法院针对该案进行了解释说明，在社会上仍然引起了对人工智能技术应用的质疑和广泛讨论。诚然，我们应当肯定人工智能技术的工具性价值，如最高人民法院委托苏州中院研发的庭审语音识别系统，可以将语音自动转化为文字，并能自动区分庭审发言对象及发言内容，法官、当事人和其他参与人均能实时看见转录文字。庭审语音识别系统在智慧法院中的应用极大地便利了书记员的记录工作。目前，语音识别正确率已达到90%以上，庭审时间平均缩短20%-30%[4]。

然而，如在本案中涉及的COMPAS系统，其机器学习算法往往涉及商业秘密，不会对公众进行公布。因此，当它在我们的生活中发挥越来越重要的决策作用时，我们通常无法控制和预测算法中是否存在歧视或某种不公平倾向。随之而来地，人工智能技术的应用也存在着准确性、算法歧视、不充分告知等风险。当企业使用算法程序为用户提供服务时，我们建议应当基于事

2.COMPAS系统的137个问题：https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html

3.Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing: https://harvardlawreview.org/2017/03/state-v-loomis/

4.最高法工作报告解读系列访谈：加快建设智慧法院：http://www.court.gov.cn/zixun-xiangqing-85042.html



当企业使用算法程序为用户提供服务时，我们建议应当基于事实作出公平、公正的决策，人工智能技术提供的分析结果不应在决策中起到唯一的决定性作用；在得出评估结果后，应对结果进行复核，或采取多种方式或模型对评估结果进行交叉验证，增强模型的精准性及可用性；充分提示用户类似机器学习系统可能存在的风险，确保操作流程公平、公正、规范，并在适度范围内向公众说明算法的基本逻辑和必要信息。另外，企业还应根据事实和时代的变化及时更新、监测算法模型，以维护机器学习算法的准确性。

实作出公平、公正的决策，人工智能技术提供的分析结果不应在决策中起到唯一的决定性作用，而应仅仅作为增强准确性的定量工具。在得出评估结果后，应对结果进行复核，或采取多种方式或模型对评估结果进行交叉验证，增强模型的精准性及可用性；充分提示用户类似机器学习系统可能存在的风险，确保操作流程公平、公正、规范，并在适度范围内向公众说明算法的基本逻辑和必要信息。另外，企业还应根据事实和时代的变化及时更新、监测算法模型，以维护机器学习算法的准确性。

（二）中国人脸识别第一案：杭州一动物园被起诉[5]

1. 案件事实

2019年4月27日，浙江理工大学副教授郭某在杭州野生动物世界办理了一张1360元的双人年卡。园方明确承诺在该卡有效期一年内通过验证年卡及指纹入园。2019年10月17日，郭某收到了来自杭州野生动物世界的一条短信：园区年卡系统已升级为人脸识别入园，原指纹识别已取消，未注册人脸识别的用户10月17日之后将无法正常入园，需要尽快携带年卡到园区年卡中心办理升级业务。

郭某认为面部特征等个人生物识别信息属于个人敏感信息，一旦泄露、非法提供或者滥用将极易危害包括原告在内的消费者的人身和财产安全。因此，2019年10月28日，郭某向杭州市富阳区人民法院提起了诉讼，要求被告确认告示和短信通知中相关内容无效、退还年卡卡费、赔偿交通费并删除原告个人信息等。被告杭州野生动物园的负责人表示，人脸识别可以有效提升消费者的入园速度。

本案于2020年6月15日开庭，将择期宣判。

2. 风险分析

本案被称为中国的“人脸识别第一案”，使新兴技术的应用和隐私保护的话题被推到了风口浪尖。目前，人脸识别在国内一方面较受争议，人们对人脸识别技术的发展水平、安全程度乃至其中涉及的信息收集、处理实践知之尚浅，另一方面，从登机、检票入口的刷脸身份验证，到公司入口的门禁系统、小区门口的快递柜刷脸取件，人脸识别技术的应用已经在国内随处可见，在某些方面可能称得上泛滥。然而，国内仍然缺失相应的法律法规或指引性文件，及人脸识别技术应用的认证标准和审核准入机制，以规制此类新技术的应用，明确人脸、声纹、虹膜等生物特征数据的收集和使用的边界。我们相信，本案的判决必将对国内监管趋势和相关企业实践产生一定的指引

5.中国人脸识别第一案 杭州一动物园被起诉：http://epaper.ynet.com/html/2019-11/04/content_340978.htm?div=-1

作用。

在现阶段，对于企业而言，我们建议企业依据最小必要原则，评估是否必要在业务中应用人脸识别技术。企业应只有在评估结果为必要时才加以采集，否则将面临较高的合规风险。在收集前，需获取数据主体的明示同意，以及应考虑如何获取数据主体的同意才能最大限度地规避法律风险。我们建议企业在内部建立完善的隐私保护制度，对日常工作中能够接触到人脸数据或其他生物特征数据的人员进行背景调查；在隐私政策中说明生物特征数据的收集、使用、存储、共享等实践，并向用户完整、充分地告知；通过弹窗展示等显著方式获取用户的授权同意。同时，企业自身也需承担更为严格的数据安全保护义务，并定期对员工进行数据隐私安全培训，增强数据安全意识。除此之外，由于民众隐私保护意识的提升，数据隐私保护领域的变化可谓日新月异，企业应密切关注行业立法与监管态势，积极跟进相关主管部门对人脸识别技术应用有关的规范出台情况，确保与自身实践相符合。

（三）瑞典一高中使用人脸识别技术监控学生出勤率被处罚[6]

1. 案件事实

2019年2月，瑞典北部的谢莱夫特奥市（Skelleftea）政府在接受瑞典电视新闻（SVT Nyheter）采访时称，该市教师每节课需要花费十分钟登记学生的出勤情况，合计每年共要花费约17280个小时。为了节省教学时间，市政府允许部分学校使用人脸识别技术对学生的出勤情况进行考察。

在该市于2018年秋季开展的名为“未来教室”（Future Classroom）的试验项目中，安德斯托普高中（Anderstorp High School）对22名学生进行了为期三周的跟踪调查，主要是为了记录下他们每次进入教室的时间。学校通过人脸识别技术，以照片的形式捕获学生们的面部生物特征数据，拍摄的照片会与学生们之前注册时提交的照片作比对，并存储在没有连接互联网的本地计算机中。存储的数据包括学生的照片和学生的姓名。

2. 裁判结果

2019年8月21日，瑞典数据监管机构（The Swedish Data Inspection Authority）裁定，安德斯托普高中的行为违反了《通用数据保护条例》（General Data Protection Regulation，GDPR）的相关规定，因此对其处以20万瑞典克朗的罚款，约合人民币14.8万元。瑞典数据监管机构的具体处罚依据如下：

（1）该学校征得的“同意”不能构成个人数据处理有效的合法性基础

6.瑞典数据监管机构裁定全文：https://www.-datainspek-tionen.se/globalas-sets/doku-ment/beslut/-facial-recognition-used-to-monitor-the-attendance-of-students.pdf

安德斯托普高中声称，在开展该试验之前，学校已经对项目的目的和会进行的数据处理活动进行了告知，并且获得了学生家长的明确同意。如果学生们不希望参与该项目，学校将沿用旧的方法记录学生们的考勤情况。学生们也被告知他们可以随时选择退出该试验项目。

但是，瑞典数据监管机构指出，根据GDPR第6.1条规定，数据主体的同意应为自由、具体、知情和毫不含糊地表示意愿的行为。另外，GDPR的前言部分第43条说明，如果数据主体与控制者之间的关系存在明显的不平衡，则同意不应被视为个人数据处理有效的法律依据。针对学校这一机构而言，很明显，学校在成绩、助学金、贷款和教育方面，甚至于未来的就业机会和学业，都对学校存在依赖关系。因此，瑞典数据监管机构认为，学校获得的同意不能有效地构成个人数据处理的合法性基础。

（2）收集方式和数据类别违反最小必要性原则

安德斯托普高中声称，使用人脸识别技术登记学生的出勤情况，与传统手工方式相比，显著提升了教师工作的效率和准确性，目前被认为是符合法律规定且满足需求的最佳方法。但是，瑞典数据监管机构认为，该学校也可以采取其他更加保护学生个人数据的方式完成监控出勤情况的目的。因此，根据GDPR第5条的规定，该高中采用人脸识别技术收集学生的生物特征数据违反了GDPR所要求的最小必要性原则。

（3）该学校未开展全面的数据保护影响评估或进行事先咨询

由于人脸识别技术是一项新技术，安德斯托普高中开展的风险评估未包含GDPR第35条第7款中规定的对于数据主体的权利和自由的风险评估，及对与处理目的相关的处理机制必要性的评估。同时，根据GDPR第36条规定，控制者应当在处理之前向监督机构进行咨询。很明显，瑞典数据监管机构并没有收到此类预先咨询。

3.风险分析

在人脸识别技术高速发展的今天，瑞典数据监管机构对于人脸识别技术作出的“第一罚”，不仅显现了数据保护监管机构对于涉及个人数据的新技术的密切关注，也许还预示着未来对此类新技术应用的监管力度和方向。

为此，对于可能涉及人脸识别技术应用的相关企业，我们建议从以下几个方面提升数据保护意识和能力，确保技术实现的全流程合法、合规：

（1）谨慎使用人脸识别技术收集生物特征数据

在使用人脸识别技术收集用户生物特征数据之前，应谨慎且全面地评估目的是否充分、必要，可以考虑除适用人脸识别技术这一方式外，是否可以

通过其他类似但干预性更小的方式实现以上目的。

(2)征得用户自由、明确作出的同意

如企业经过评估，确定将应用人脸识别技术收集生物特征数据，应确保征得用户的授权同意。此处，需特别注意的是，该同意需为用户主动、自愿作出的同意，如双方的关系存在一定的不平衡性，则可能影响到同意的有效性。同时，企业也需通过隐私政策或者其他方式如弹窗告知等，具体且完整地告知用户此类数据收集的目的、方式、范围等。

(3)在人脸识别技术应用之前，开展数据保护影响评估

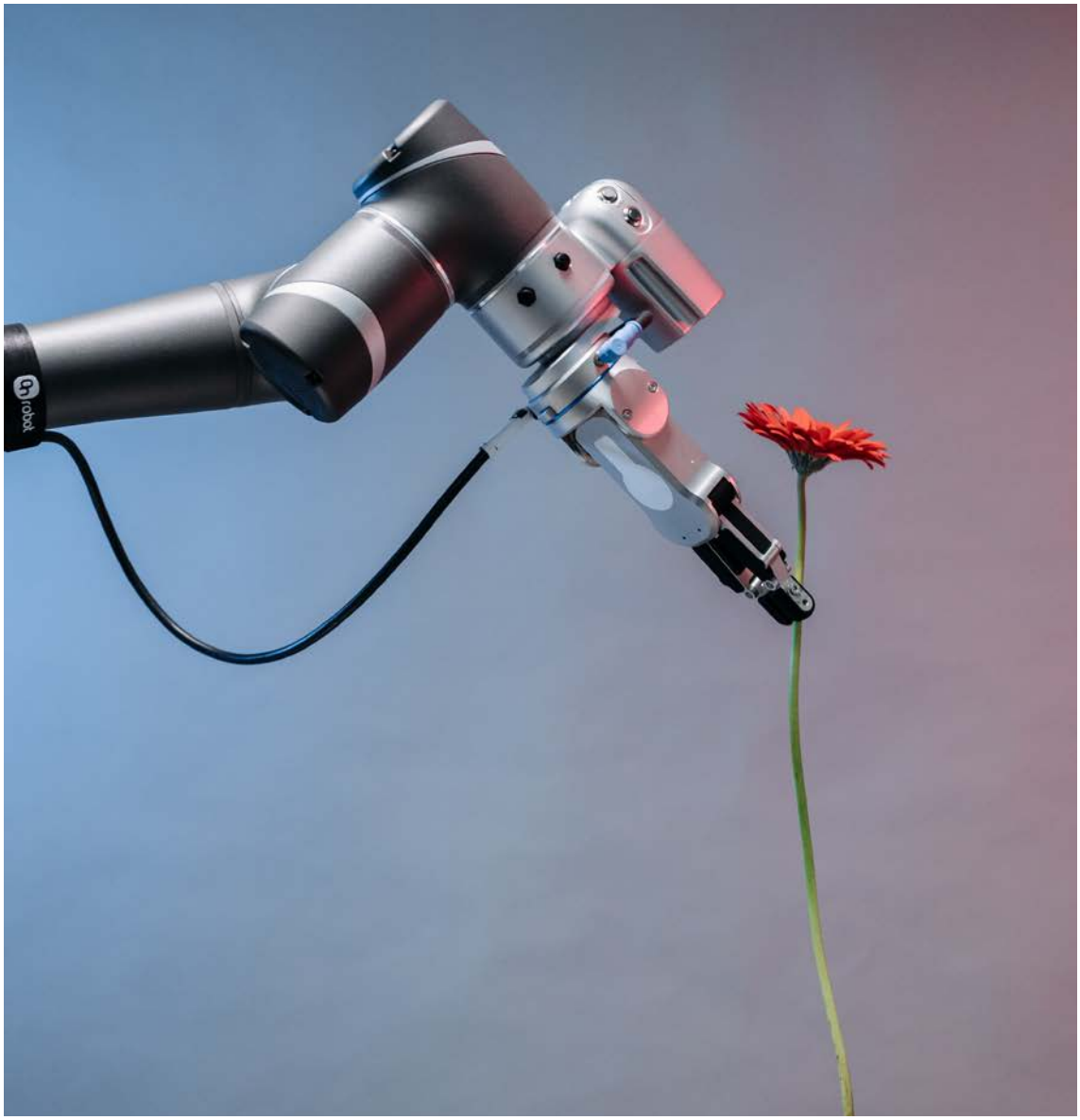
在人脸识别技术应用之前，应对使用人脸识别技术对数据保护的影响进行评估。在当地法律需要的情况下，应向数据保护监管机构提供相关材料进行预先咨询。

(4)提升数据保护安全能力

企业应在确保数据收集、处理实践合法、合规的同时，注意提升自身的数据保护安全能力，如对收集的生物特征数据仅存储摘要信息、设定访问权限控制措施和流程制度建设、对数据收集和处理实践进行记录并定期进行安全审计、加强对员工的安全意识培训和安全能力考核等，严防数据泄露，保证数据安全。

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

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



人工智能语境下GDPR的挑战及中欧数据保护异同点分析

作者/ 陈际红、韩璐、DR. DENNIS-KENJI KIPKER

第四次工业革命时代，人工智能领域成为必争之地。作为新时代企业发展的石油，数据对于人工智能行业发展而言发挥着基础资源及助推器作用。世界各法域陆续更新立法，加强对数据的保护。这其中，欧盟于2018年5月开始实施的《通用数据保护条例》（General Data Protection Regulation，“**GDPR**”），构建起了欧盟数据保护新的立法框架。因其扩张型的域外适用效力与严格的法律责任，GDPR也成为数据保护领域的先导者。本文拟通过对GDPR的系统梳理，兼评中欧数据保护的异同点，探索在人工智能技术开发领域企业与开发者如何合法合规合理使用数据，以供从业者参考。

PART 01
GDPR及数据保护法律框架概述

自2018年5月25日生效以来，GDPR构建起了欧盟数据保护新的立法框架。GDPR生效后，代替了欧洲议会和理事会1995年10月24日关于个人数据处理的个人保护及此类数据自由流动的第95/46/EC号指令。与欧盟法规相比，欧盟指令对成员国没有直接约束力。此外，欧盟成员国有义务将指令原则转化为各自的国内法。因此，欧盟各成员国以不同方式止执行该指令，各成员国之间的数据保护水平变得部分不平等和不一致，导致在欧盟运营的公司的法律不确定性和不透明性。GDPR通过保证欧盟内各成员国对自然人一致高水平的保护，并消除在欧盟内个人数据流动的障碍来解决此问题，同时还规定在所有成员国中就个人数据处理活动对每个自然人权利和自由的保护程度应相等。与保护网络空间和国家安全的《中华人民共和国网络安全法》（以下简称为“**《网络安全法》**”）相比，GDPR仅关注自然人的人格权和财产权利。

GDPR与《网络安全法》的另一个区别在于：中国的数据保护法律框架主要由一项核心法律为主，辅之以若干法律规范和技术标准，而欧盟数据保护法律框架则建立在各种法律规范之上，大多基于若干分支和主题的特定法规，其中部分法规可由欧盟各成员国定义。根据GDPR中的“开放条款”，各成员国可自行定义管理数据保护框架中的部分内容。由于这一部分内容往往由国家特别法处理，使得欧盟数据保护框架的建立相较于GDPR本身的政治意图而言更加困难和不明确。举例来说，数据控制者可以基于履行法定义务所必要而处理个人数据。针对此类法定义务，成员国可制定更加详细具体的规定，以保证对数据的合法公平处理。例如德国，与法定健康保险合作的医

生和医院，如为保障健康所必要则有义务处理病人的数据。由于此项规定，数据控制者必须遵守除欧盟法律外所适用的特定国家的法规，以实现充分合规。

关于欧盟的数据保护框架，除GDPR以外，还必须提到《电子隐私指令》（以下简称“**《指令》**”）。该项《指令》为处理通过电子形式和通信服务传输的个人数据提供了具体而严格的保护规则。根据GDPR第95条，对于《指令》中已经施加特殊责任的事项，GDPR不应再对同一事项再向自然人或法人施加额外责任。2020年，《电子隐私条例》本计划替代已略过时的《指令》：《电子隐私条例》本可以与GDPR同时成为法律，但由于严重的政治争端导致欧盟推迟了对新法律的审议。《电子隐私条例》草案与《指令》相比，扩大了适用范围，并对“顶级通信服务”产生影响，即互联网中无需运营通信基础设施的通信服务提供商，例如电子邮件或信息服务提供者。如果《电子隐私条例》正式通过，则将替代《指令》，同时所有对于《指令》的引用均会影响该条例。至于与GDPR之间的关系，尽管《电子隐私条例》草案中声称已就GDPR中的通用条款进行了澄清和说明，但关于《电子隐私条例》的适用范围及生效时间等仍存在诸多不确定性。

PART 02

GDPR如何保护个人数据

2.1 个人数据保护关键词

(1)个人数据

根据GDPR第4条，个人数据是指与已识别或可识别的自然人（数据主体）相关的任何数据。可识别的自然人是指通过姓名、身份证号、定位数据、网络标识符号以及特定的身体、心理、基因、精神状态、经济、文化、社会身份等识别符能够被直接或间接识别到身份的自然人。

在中国数据保护法律框架下，《网络安全法》中对个人信息的定义为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，包括但不限于自然人的姓名、出生日期、身份证号码、个人生物识别信息、住址、电话号码等。同时，配套的《GB/T 35273-2020信息安全技术 个人信息安全规范》中对个人信息的判定方法及类型进行了详细的说明，所有能够识别到特定自然人或与其他信息相关联可以识别到特定自然人的信息均可能被判定为个人信息。

(2)特殊类别的个人数据

根据GDPR第9条，特殊类别的个人数据是指可以显示种族或民族、政治观念、宗教、哲学信仰或工会成员身份的个人数据、基本数据、为识别特定自然人的生物识别数据以及和健康、个人性生活或性取向相关的数据。GDPR原则上禁止对特殊类别的个人数据进行处理。

中国数据保护法律框架下类似的概念为个人敏感信息，指任何一旦泄露、非法提供或者滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。相较于GDPR项下的特殊类别的个人数据，中国数据保护法律框架下的个人敏感信息覆盖范围更广。

(3)数据控制者和处理者

根据GDPR第4条，数据控制者是指能够单独或共同决定个人数据处理目的与方式的自然人、法人、公共机构、行政机关或其他非法人组织。数据处理者则是指为控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织。

中国数据保护法律框架下个人信息控制者及处理者的概念与GDPR基本相同，控制者均是指有能力决定个人信息处理目的、方式等的组织或个人，处理者则是在是控制者指示下进行个人信息处理活动的组织或个人。

PART 03

您的企业是否落入GDPR的管辖

判断是否落入GDPR的管辖是实现GDPR合规的起点。在判断过程需同时考虑实质范围及地域范围的要求。

3.1 实质范围

根据GDPR第2条，GDPR适用于全自动、半自动个人数据处理，以及形成或旨在形成用户画像的非自动个人数据处理，即GDPR适用于个人数据处理活动。若您的企业所进行的数据处理活动不涉及个人数据，则可能不会落入GDPR的管辖。

3.2 地域范围

地域范围的判断有两种标准：经营场所标准、目标指向标准。

其中，经营标准是指根据GDPR第3条第1款，在欧盟境内设有经营场所的数据控制者或数据处理者，只要个人数据处理活动发生在经营场所开展

活动的场景下，即使实际的数据处理活动不在欧盟境内发生，该数据处理活动也要受GDPR管辖。

目标执行标准则是指根据GDPR第3条第2款，GDPR适用于在欧盟境内无营业场所的数据控制者或处理者施行的针对欧盟境内数据主体的下述个人数据处理活动：(a)向欧盟境内的数据主体提供商品或服务，无论是否要求数据主体支付价款；(b)对欧盟境内数据主体的行为进行监控。

相较于GDPR管辖的判断标准，在中国数据保护法律框架下，在中华人民共和国境内建设、运营、维护和使用网络以及网络安全的监督管理，应当遵守《网络安全法》的各项要求。

PART 04

如何规范地收集与处理个人数据

4.1 处理个人数据的原则

与中国数据保护法律体系类似，GDPR同样确定了处理个人数据的基本原则，各项个人数据处理活动均应按照合法性、公平性、透明性、目的限制、数据最小化、存储限制、完整性和保密性以及可问责的原则执行。对于数据控制者及处理者而言，遵守处理个人数据的基本原则是法定义务而非最优选择，若违反数据处理基本原则的要求即会受到相应的处罚。GDPR第5条对处理个人数据的各项基本原则进行了详细的说明。

(1)合法性、公平性和透明性原则

数据控制者及处理者对于个人数据进行的各项处理活动均需具备适当的法律基础。此外，还必须使数据主体能够以简单、清晰易懂的方式了解对其个人数据进行处理的情况，包括数据控制者的身份、数据处理的目的、处理的数据类型、相应的风险、适用的法律法规、控制者作出的保证以及可能对个人数据主体权利造成的影响等。

(2)目的限制原则

数据控制者及处理者收集个人数据必须出于明确、清晰和合法的目的，且对个人数据的处理不得超出收集时所明确的目的。如果数据控制者需对个人数据进行进一步处理，必须保证所进行的处理活动与原始处理目的相兼容。如果数据控制者想要变更数据处理活动的目的(例如在线上购物的场景下，收集个人数据是为了完成交易/履行合同，现计划将此类数据用于个性化广告)，必须保证新的数据处理活动同样具备相应的法律基础。

(3)数据最小化原则

数据控制者及处理者收集个人数据的范围应当仅限于为实现目的所必需的范围内，对个人数据所进行的处理活动应当保证为实现目的所必需的最低程度。

(4)准确性原则

数据控制者及处理者应当保证被处理的个人数据应当是准确的，且在必要时应当对个人数据进行更新。如出现数据不准确的情形，应当采取一切合理措施以确保及时删除或更正不准备的个人数据。

(5)限期存储原则

数据控制者及处理者应当保证可识别到特定个人的个人数据的存储时间不应超过实现处理目的所必要的时间。数据控制者及处理者应当制定数据存储政策，明确规定根据数据保护法律法规可以存储哪些数据、以何种形式进行存储、可以存储多久等问题。

(6)完整性与保密性原则

数据控制者及处理者应当采取适当的技术和组织措施以充分保障个人数据安全，防止对个人数据进行未经授权的访问或非法的处理，或发生意外毁损、灭失等。

(7)可问责性

数据控制者及处理者在处理个人数据时应当充分遵守以上各项原则，同时还必须以各种可举证的形式证明所进行的数据处理活动符合GDPR的要求。

4.2 处理个人数据的法律基础

如前所述，个人数据处理活动应当以合法的方式进行。在GDPR项下，仅在具备适当法律基础的情形下，方可进行个人数据处理活动。与中国数据保护法律框架下数据处理的主要依据个人信息主体的同意不同，GDPR项下数据处理活动的法律基础不仅只有数据主体的同意。根据GDPR第6条的规定，个人数据处理活动所依据的法律基础主要有六种，可分为以下两类。

(1)个人数据主体的同意

GDPR项下的同意是一项非常重要的、有详细要求的法律基础，有效的同意需是个人数据主体自由作出的、具体的、建立在知情基础上的、同意处理与其有关的个人数据的明确意思表示。数据控制者以个人数据主体的同意作为数据处理活动所依据的法律基础的，应当证明其以取得了数据主体的同意（尤其是在在线服务的场景下）。数据主体的同意可以通过口头、书面

或电子等各种形式作出，只要保证能够明确表达数据主体的意思表示即可。因此，数据主体作出的某项明确的具体动作也有可能构成同意。

此外，同意应当是由数据主体主动作出的，这意味着如果数据主体实际上无其他选择或者拒绝同意或撤回同意将会使其处于不利地位，同意就不是主动作出的。当评估某项同意是否是由数据主体自由作出时，应当最大限度地考虑是否是以数据主体的同意作为履行合同的必要条件，不得将个人数据主体必须同意作为履行合同的一项捆绑条件。另外，根据GDPR第7条中对于同意的定义，同意应当是由数据主体在充分知情的基础上作出。数据主体至少应当知悉数据控制者的基本信息以及处理其个人数据所要实现的目的。数据控制者还应当在数据主体作出同意之前告知其享有随时撤回其同意的权利，并保证数据主体撤回同意的方式与其作出同意的方式一样简单。

关于同意的另一个关键问题为儿童的同意。由于缺乏认知能力，儿童很难基于其个人的充分认知作出自由的意思表示。根据GDPR第8条，作出有效同意的最低年龄限制为16岁。如果儿童的年龄小于16岁，只有其父母或监护人作出同意，数据处理活动才能合法进行。数据控制者应当结合技术可行性采取合理的措施，确保此类情形中对儿童具有监护责任的主体确已作出同意。同时，成员国法律可就儿童的同意作出特殊规定。

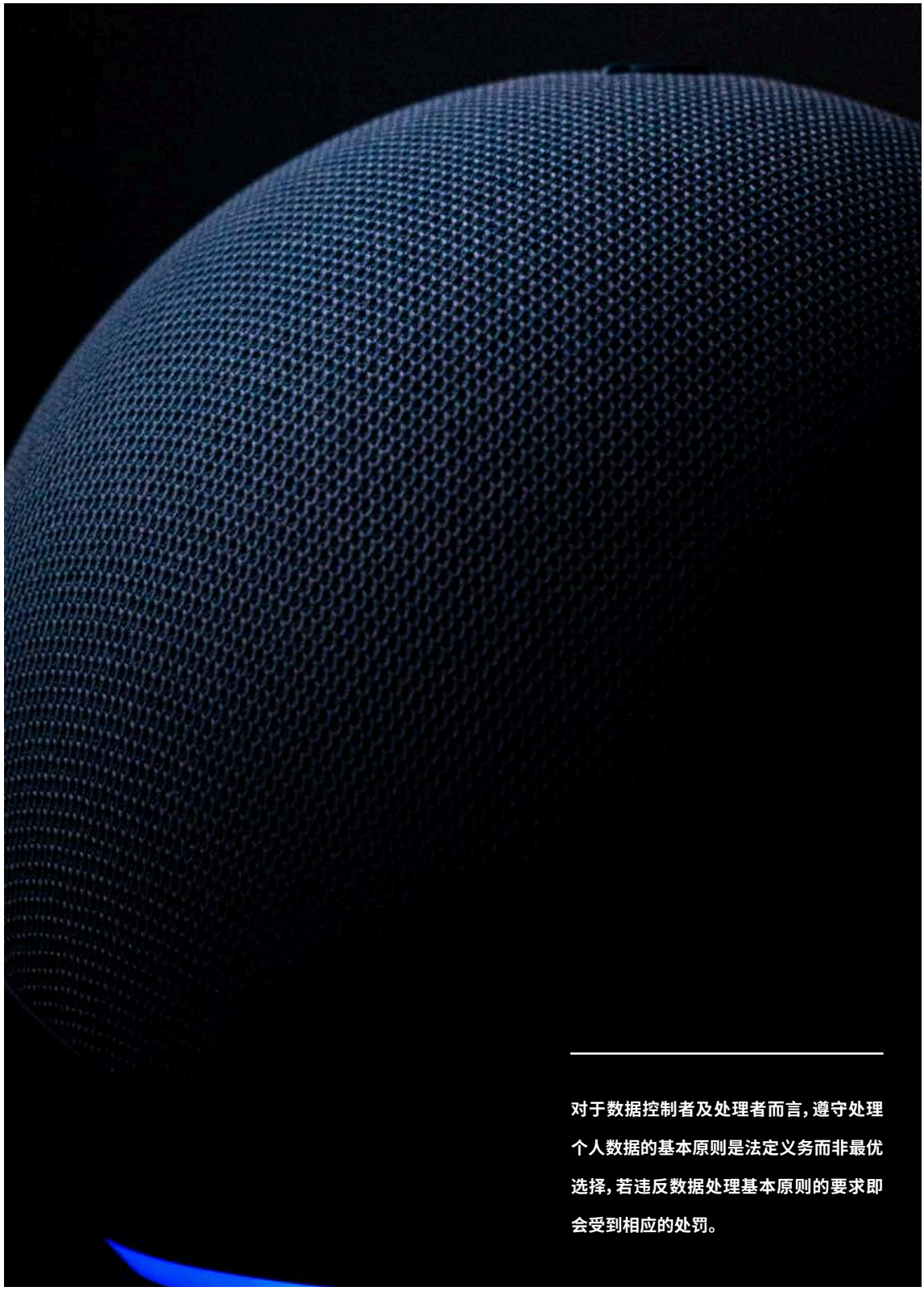
(2)其他法律基础

根据GDPR第6条，除数据主体的同意以外，数据处理活动还可基于以下几种法律基础进行：

◆**履行合同所必要，**即数据处理活动是为了履行数据主体为一方的合同。根据GDPR第6条第1款(b)项，若数据处理活动是在签订合同前基于数据主体的请求所进行的，也属于该项法律基础所包括的情形。判断是否可适用履行合同所必要作为数据处理活动，应当根据合同条文及数据处理活动的目的等来判断“必要性”。仅在不进行数据处理活动就无法履行合同时，才能称之为必要。例如经营在线商店的经营者至少需处理客户的姓名、地址、支付信息等数据，才能履行与客户之间的购买合同。

◆**履行法定义务所必要，**即数据处理活动是数据控制者履行其所受约束的法律法规规定的义务所必需的。此处所指的义务不是私人自主决定的义务，而是欧盟法律或成员国法律中所规定的法律义务。

◆**保护重大利益所必要，**即数据处理活动的进行是为了保护数据主体或另一自然人的重大利益。此条款主要针对紧急情况而制定，但是这并不意味着只有在出现死亡风险的情况下才能够适用。以此项法律基础为依据的数



对于数据控制者及处理者而言，遵守处理个人数据的基本原则是法定义务而非最优选择，若违反数据处理基本原则的要求即会受到相应的处罚。

据处理活动主要是指医疗紧急情况、流行病监测或自然灾害等。

◆**保护公共利益所必要,**即数据处理活动是数据控制者为了公共利益或基于官方权威而履行某项任务而进行的。此条款旨在允许公权力机构进行数据处理活动,对个人或其他组组织没有重大意义。

◆**正当利益,**即数据处理活动对于数据控制者或第三方追求的正当利益是必要的。在此种情形下,需保证数据控制者所追求的正当利益不会影响数据主体的基本权利和自由。数据控制者应当承担相应的举证责任。正当利益的衡量一方面要考虑数据处理活动的目的,另一方面也要充分考虑对受影响的主体所造成的干预程度。进行数据处理活动的措施对数据主体的干预程度越高,数据主体的基本权利和自由越优于数据控制者的利益。其中,特殊类别个人数据由于其高度的敏感性,一般来说,对其的保护优于数据控制者的各项利益。

4.3 特殊类别个人数据的保护

相较于一般类型的个人数据,对特殊类别个人数据进行处理需遵循更加严格的要求。根据GDPR第9条,特殊类别个人数据是指能够揭示种族或民族背景、政治观念、宗教、哲学信仰或工会成员身份,以及遗传数据、用于识别特定个人的生物识别数据、有关健康或自然人性生活、性取向的数据。GDPR原则上禁止对特殊类别个人数据进行处理,仅在以下有限的例外情形下可以处理:

◆**同意,**此处的同意必须是数据主体针对特定的个人数据作出的、符合GDPR关于同意要求的明示同意。

◆**劳动法或社会法,**即数据处理活动对于保障数据主体可行使其在劳动法、社会保障法等项下的权利是必要的。

◆**保护重大利益,**即数据主体因为物理或法律原因无法作出同意的意思表示,但是数据保护活动对于保护数据主体或其他自然人的重大利益是必要的。

◆**已明显公开的数据,**即可以对数据主体已经明显公开的相关个人数据进行处理。

◆**法律主张,**即数据处理活动对于提起、形成法律主张或进行抗辩是必要的,或对于法院进行司法活动是必要的。在此情形下,数据控制者或处理者需谨慎地进行利益平衡。

◆**研究目的,**即根据欧盟或各成员国法律,数据处理活动对于实现科学、历史或统计目的是必要的。

PART 05

GDPR赋予数据主体哪些权利

GDPR项下数据主体所享有的权利与《网络安全法》项下的主体权利差别相对较小。根据GDPR，数据主体所享有权利包括知情权、访问权、更正权、删除权（或称被遗忘权）、可携带权、限制处理权、反对权以及免受自动化决策约束的权利。

5.1 知情权

数据控制者在收集个人数据之前，应当向数据主体告知数据处理活动的相关信息。根据个人数据来源的不同，GDPR区分了告知的不同方式：在直接从数据主体处收集个人数据的情形下，应当适用GDPR第13条的规定，直接向数据主体提供相关信息。在不直接从数据主体处收集个人数据的情形下，应当适用GDPR第14条的规定在获得个人数据后一段合理期限内提供相关信息。

数据控制者应当向数据主体告知的信息包括控制的身份与详细联系方式、代表的姓名（如适用）、数据保护官的详细信息（如适用）、数据处理的目的、数据处理所依据的法律基础、个人数据的接收者（如有）、跨境传输的相关情况、数据的存储期限、数据主体所享有的权利、撤回同意的权利、提供个人数据的法定或合同义务、自动化决策的相关情况等。

5.2 访问权

数据主体所享有的访问权旨在提高数据处理活动的公正性和透明度，为数据主体验证对其个人数据进行处理的数据处理活动的合法性提供了可能。任何数据主体均享有访问权，即使数据控制者处并无权利请求人的任何数据，也应当告知其这一事实情况。如果数据控制者处有权利请求人的数据，则应当向其提供所存储的其个人数据的副本。

数据主体可访问的至少包括以下信息：数据处理的目的、处理的个人数据类别、数据将被披露/正在被披露的接收人（特别是位于第三国的接收人）、存储期限或确定存储期限的标准、向监管机构投诉的权利、自动化决策的预期结果、个人数据跨境传输的情况等。在向数据主体提供上述数据的副本时，如有数据主体是以电子格式提出权利请求，数据控制者也应当以电子格式向其提供相关信息。

5.3 更正权

鉴于错误的信息有可能导致对个人数据主体虚拟数字形象的错误判断，进而对数据主体的个人发展及公众认识产生不利影响，确保所处理的个人数据的准确性具有十分重要的意义。为避免此类情况，GDPR项下赋予了个人数据主体随时要求数据控制者更正错误的个人数据的权利。同时，数据主体还有权完善数据控制者所存储的不完整、不充分的个人数据。数据库是否充分需根据具体情况进行判断，如果所缺少的数据是为了达到收集时的目的所必需的，则数据控制者必须应数据主体的权利请求在数据库中进行补充。

5.4 删除权/被遗忘权

（1）删除权

数据控制者有义务应个人数据控制者的权利请求删除其个人数据。对个人数据的删除必须以确保无法还原的方式进行，因此，将个人数据移除至系统回收站或不再允许浏览信息方式无法满足此要求。若出现如下情形，数据控制者即有权要求删除其个人数据：

◆个人数据对于实现其被收集或处理的相关目的不再必要；

◆个人数据主体已撤回其同意，且无其他适当的法律基础；

◆个人数据主体反对处理其个人数据，且没有正当理由可以继续处理；

◆存在非法处理个人数据的情形；

◆为履行欧盟或成员国法律下数据控制者所应承担的义务，个人数据需被删除。

若数据处理活动是为以下情形下所必须要进行的，个人数据主体的删除权不适用：

◆为了行使表达自由和信息自由的权利；

◆数据控制者基于欧盟或成员国的法律要求，执行基于公共利益的任务，或基于官方权威履行某型任务；

◆为保护公共健康领域的公共利益；

◆为实现公共利益目的、科学或历史研究目的或统计目的；

◆为了提起、行使或辩护法律主张等。

除非不可能实现或需付出不成比例的成本，数据控制者必要向已向其披露过个人数据接收者通知个人数据更正或删除的相关情况。同时，数据控制者应当应个人数据主体的要求告知其删除接收者的相关情况。

（2）被遗忘权

当数据控制者已经公开个人数据并且负有删除个人数据的义务时，应当

充分考虑可行的技术与执行成本，采取包括技术措施在内的合理措施通知其他数据控制者关于个人数据主体要求删除与个人数据相关的链接、备份或副本的相关情况。被遗忘权尤其适用于网络内容发布的情形，即使超出GDPR适用范围，发布者也有责任向数据处理者通知受影响数据的相关情况。

以下为被遗忘权适用情形的典型示例：数据控制者在其网站上发布了某个自然人的个人数据。通过在搜索引擎中输入姓名即可查找到相关信息，这意味着有无法控制数量的人员可访问到此个人数据，构成法律意义上的发布。若个人数据主体行使其被遗忘权，数据控制者必须通过适当的措施通知搜索引擎运营商以实现此项权利请求。同时，发布者应当承担相应的举证责任。

5.5 限制处理权

若个人数据主体要求限制对其个人数据进行处理，数据控制者则仅在有限的情形下才能继续对个人数据进行处理。若出现以下情形，个人数据有权要求限制处理其个人数据：

◆个人数据主体对于其数据的准确性存在争议，给与数据控制者一定的时间以核实个人数据的准确性；

◆数据控制者对个人数据进行非法处理，同时个人数据主体反对删除其个人数据的，可以要求对使用其个人数据进行限制；

◆个人数据对于实现其被收集或处理的相关目的不再必要，但个人数据主体为了提起、行使或辩护法律主张而需要该个人数据；

◆个人数据主体行使其反对权，需要确定数据控制者是否有由于个人数据主体合法权益和基本自由的正当理由。

在上述情形下，除非数据控制者已经征得个人数据主体的同意，或是为了公共利益、保护另一自然人或法人的权利以及为了提起、行使或辩护法律性主张等，数据控制者需暂停对个人数据所进行的处理活动。

5.6 可携带权

基于数据可携带权，GDPR通过使个人数据从一个IT环境到另一个IT环境之间的移动、传输或复制实现服务提供者的轻松切换。GDPR规定了在数据处理活动是基于个人数据主体的同意或履行合同所必要的法律基础情形下，数据主体可以以结构化的、普遍使用的和可机读的方式获得其提供给数据控制者的个人数据，并且有权无障碍地将此数据传输给另外一个数据控制者。如果技术可行，数据主体有权要求个人数据直接从一个数据控制者传

输给另一个数据控制者。举例来说，某社交网络的运营者收到用户的请求，要求将其个人数据（包括姓名、电子邮件地址、年龄、居住地、照片、评论、聊天记录等）转移至另一个社交网络的运营者。根据GDPR关于可携带权的规定，该公司应当转移该类个人数据；然而，由于部分数据（例如聊天记录）涉及到第三方的权益，可能无法转移给第三方的网络运营者。

5.7 反对权

反对权不是终止非法处理个人数据活动的权利，其目的在于结束对个人数据的依法处理活动。根据所处的具体情形，数据主体有权对基于公共利益或正当利益进行个人数据处理活动提出反对。在数据主体提出反对的情形下，除非数据控制者能够证明有高于个人数据主体的利益、权益和自由的合法利益或是为了确立、行使或辩护法律请求的合法利益，否则即应当停止对个人数据的处理活动。同时GDPR还规定了数据主体可以反对以直接营销为目的的数据处理活动。数据控制者有义务在收集个人数据之初即明确提示个人数据主体有权反对对其个人数据进行处理。

5.8 免受自动化决策权

个人数据主体有权反对数据控制者完全依靠对个人数据进行自动化处理，即对数据主体作出具有法律影响或类似严重影响的决策。此种权利的实现同样存在例外情形，当决策是建立在个人数据主体同意的基础上，或是为了履行与个人数据主体之间的合同所必要，或者决策是欧盟或成员国法律所授权的，同时所处理的个人数据不涉及特殊类别个人数据时，数据主体行使此项权利得不到相应的支持。

PART 06

数据控制者和数据处理者有哪些主要的法律义务

6.1 通用要求

（1）数据保护官

当数据控制者及处理者所进行的数据处理活动涉及大规模地对个人数据进行常规和系统性的监控或涉及对特殊类别个人数据或与刑事定罪犯罪相关数据的大规模处理，应当设立一名数据保护官（Data Protection Officer，“**DPO**”），负责处理与个人数据保护相关的问题。数据控制者或处理者应当为数据保护官履行其职责提供必要的资源以保证其可访问个人数据处

理活动及维护专业能力，进而更好地执行各项任务。此外，数据控制者及处理者应保证数据保护官的中立地位，确保其不会收到来自数据控制者或处理者有关执行任务的指示，并且不会因为履行义务被解雇或处罚。数据保护官应直接向数据控制者或处理者的最高管理层进行汇报。数据保护官应完成如下任务：

◆告知数据控制者及处理者及其进行数据处理活动的员工所应履行的欧盟及成员国法律所规定的义务；

◆根据数据控制者及处理者的个人数据保护政策，包括职责分配、意识培训及相关审计等，监测数据控制者及处理者对于GDPR、欧盟及成员国法律的遵守状况；

◆对数据控制者及处理者所进行的数据保护影响评估提供建议；

◆配合监管机构工作；

◆在与数据处理活动相关的事项及事先咨询中作为数据控制者及处理者与监管机构的联络人。

（2）欧盟代表

对于在欧盟境内无经营场所，但因向欧盟境内个人数据主体提供商品或服务或涉及对欧盟境内个人数据主体进行监控而适用GDPR的数据控制者及处理者，应当在欧盟境内委任一名代表。与中立的数据保护官不同，欧盟代表主要负责进行以下工作：

◆在欧盟境内代表数据控制者及处理者履行GDPR合规义务；

◆根据数据控制者及处理者的授权内容履行其职责；同时

◆保留所代表数据控制者及处理者进行个人数据处理活动的记录。

（3）数据处理活动的记录

数据控制者及处理者应保持其所负责的数据处理活动的记录，并且保证创建和保持记录的方式能够使监管机构在必要时访问数据处理活动的相关信息。数据处理活动记录应当至少包括以下信息：

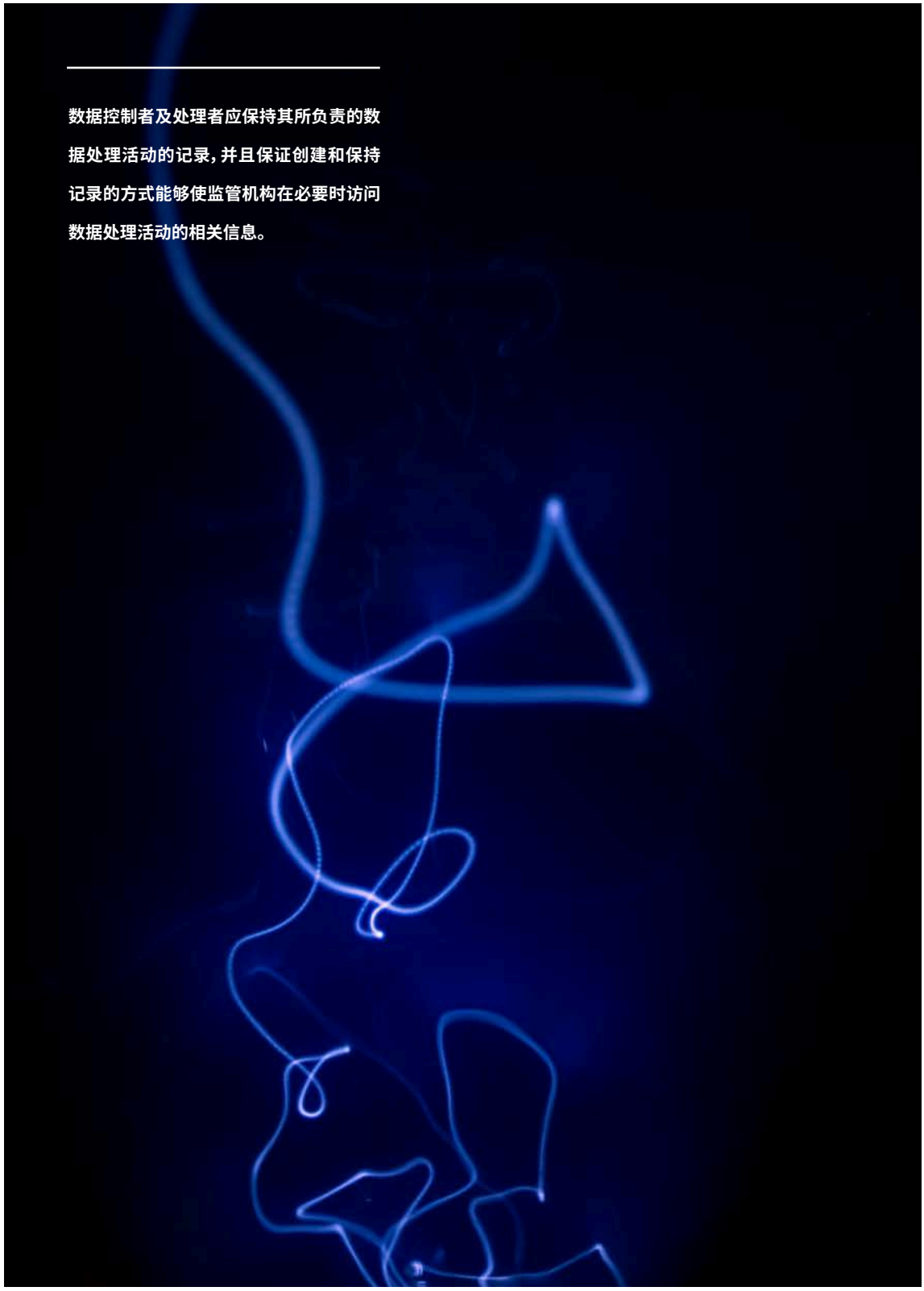
◆数据控制者的名称、联系方式以及联合控制者（如有）、代表（如有）、数据保护官（如有）的姓名及详细联系方式等；

◆数据处理活动的目的；

◆数据主体的类型及个人数据的类型；

◆个人数据已经被披露或将被披露给的接收者，以及位于第三国或国际组织的接收者的相关信息；

◆如适用，将个人数据传输至第三国或国际组织的相关情况，以及跨境传输所适用的传输机制的情况；



数据控制者及处理者应保持其所负责的数据处理活动的记录，并且保证创建和保持记录的方式能够使监管机构在必要时访问数据处理活动的相关信息。

◆如适用，针对不同类型的个人数据所设定的存储删除期限；

◆如适用，对所采用的技术和组织措施的描述。

（4）数据保护影响评估

如果数据处理活动可能会对个人数据主体的基本权利和自由带来高风险时，应当在进行数据处理活动之前进行数据保护影响评估（Data Protection Impact Assessment，**“DPIA”**），并应在进行评估时征求数据保护官的建议。数据保护影响评估涵盖了对个人数据处理活动进行准备至产生影响的全流程。根据GDPR，在以下典型场景下需进行评估：

◆涉及对个人数据进行系统、全面的评估分析；

◆涉及对特殊类别的个人数据进行处理；

◆涉及对公共区域进行视频监控；

◆涉及对区域、国家或跨国级别的大量个人数据处理记录。

除上述典型情形以外，若涉及使用自动化处理技术处理个人数据、对儿童的个人数据进行处理、对不同来源或不同数据库的个人数据进行汇集处理等情形时，也应当进行评估。

评估至少应当包括：

◆**数据映射：**对数据处理活动进行系统梳理，并说明数据处理活动的目的及所依据的法律基础；

◆**必要性评估：**评估数据处理活动及目的之间的必要性及比例性；

◆**风险评估：**评估可能给个人数据主体的基本权利和自由带来的风险；

◆**措施描述：**考虑到个人数据主体及其他涉及自然人的基本和权利，所采取的风险应对措施，包括安全保障措施及相关证明机制等。

（5）设计和默认的隐私保护（Privacy by Design and by Default，“PbD”）

根据GDPR的要求，无论是在设计数据处理活动之初决定处理的目的及方式时，还是在数据处理活动全流程中，均需履行设计和默认的数据保护义务以实现持续合规。

◆设计的隐私保护

在数字时代，如果没有符合隐私合规要求的技术设计，很难实现充分的隐私保护，因此数据控制者有义务在设计数据处理活动时即采取充分的隐私和安全保障措施。数据控制者应当在综合考虑技术的先进性、实施成本、个人数据处理活动的性质、范围、内容和目的等因素以及可能给自然人基本权利和自由造成的风险程度的基础上，在设计数据处理活动之初以及在进行个人数据处理活动的全过程中均应采取适当的技术和组织措施（TOM）有

效地履行各项数据保护基本原则，并在处理中采取必要保障措施以满足GDPR的要求并保护个人数据主体的权利。同时，这也意味着不能在数据泄露事件发生之后才采取技术和组织措施。

技术措施为与数据处理活动相关的技术程序、安排等，例如删除数据载体，为防止未经授权的人员访问的结构措施为安全措施，例如软硬件检查、访问控制、加密或密码安全等。组织措施则主要针对技术程序设计的外部框架，例如进行活动记录和取样程序等。以一个成功的隐私设计为例，其中包括保护安全用户身份验证解决方案、匿名化和假名化、集成加密方法、数据最小化以及车联网领域特殊的标识和内容数据的分离等。

◆**默认的隐私保护**

默认的隐私保护是指数据控制者承诺采取适当的技术和组织措施以确保在默认情况下仅处理为实现提供目的所必需的数据。基于此，个人数据主体无需更改隐私设置即可获得最高级别的隐私设置。此项义务适用于所收集的个人数据的数量、处理个人数据的程度、存储期限及可访问性。如果用户希望处理其个人数据，其需独立更改设置。根据默认的隐私保护，此类设置应当以主动勾选的方式完成，以确保受影响的个人数据主体充分知悉其个人数据被处置的情况。

(6)数据泄露的通知

若发生个人数据泄露，数据控制者有义务及时向监管机构报告并在可能给个人数据主体的基本权利和自由造成高风险时通知涉及的个人数据主体。在可行的情况下，除非个人数据泄露不太可能对个人数据主体的基本权利和自由造成风险，数据控制者应当在知悉泄露事件发生后的72小时内向监管机构进行报告。包括的内容至少应当包括：

◆个人数据泄露的性质，包括在可能的情况下，涉及的个人数据主体的类型及大致数量，涉及的个人数据的类型及大致数量；

◆数据控制者、数据保护官或其他知情联系人的姓名及详细联系方式；

◆个人数据泄露可能造成的后果；

◆数据控制者为解决个人数据泄露或减轻不利影响而采取或将要采取的措施。

若数据处理者发生个人数据泄露，应当以同样的方式及时通知数据控制者。

6.2 对数据处理的实质性要求

基于上述基本义务，数据控制者及处理者进行数据处理活动时，需满足

的实质性要求可以概括为：

◆对个人数据进行的任何处理活动均需具备适当的法律基础，并满足GDPR各项数据处理基本原则的要求；

◆如涉及到数据跨境传输，除具备法律基础、满足原则要求以外，还需采取适当的传输保障机制；

◆上述基本要求的实现，需要得到内部的技术管理措施、流程和制度的保障，亦需通过对外公示的隐私政策、隐私设置等实现。数据控制者及处理者应谨慎地根据业务模式、数据流向以及面向的用户群体对数据处理动作进行梳理和分类，确保具备适当的法律基础及适宜的呈现方式以达到GDPR的要求。

6.3 共同控制者和数据处理者的义务

(1) 共同控制者

当两个或者多个数据控制者联合共同决定数据处理活动的方法及目的时，即构成共同控制者。在此种情形下，共同控制者之间应当以透明的方式明确遵守GDPR合规要求的相应责任，尤其是要明确对个人数据主体权利行使的保障。

为保证个人数据主体的合法权益，共同控制者应当采取适当的方式使个人数据主体知悉共同数据控制者之间的责任划分安排。此外，根据GDPR的规定，不论共同数据控制者之间作出何种约定，个人数据主体均可以向其中任一数据控制者主张其根据GDPR所享有的权利。

(2) 数据处理者

当数据控制者需要数据处理者代表其进行数据处理活动时，数据控制者所选用的应当是有充分保证可采取适当技术和组织措施的、针对个人数据的处理方式充分符合GDPR的各项要求并且可保障数据主体权利的数据处理者。如果一项数据处理活动对数据控制者而言过于复杂或过于广泛，委托数据处理者进行处理可以在一定程度上简化数据控制者的数据处理活动，但数据控制者应当针对外包流程制定严格的数据保护措施。因此，数据控制者的商业利益与个人数据主体权益之间应当达到一种适当的平衡。若数据控制者选择将其数据处理活动外包，其必须确保数据处理者的处理活动受合同或其他欧盟或成员国法律的约束，该类约束应当明确以下内容：

◆数据处理活动持续的期限；

◆数据处理活动的性质及目的；

◆所涉及个人数据的类型及个人数据主体的类型；

◆数据控制者的权利义务；

◆除非欧盟或成员国法律另有规定，数据处理者应当仅按照控制者的书面指示进行处理活动；

◆数据处理者确保有权进行数据处理活动的人员已承诺保密或负有法定的保密义务；

◆遵守数据安全要求；

◆未经数据控制者书面允许，数据处理者不得为自己或为数据控制者另行委托其他数据处理者。如有数据处理者经允许委托了其他数据处理者，应当确保已采取相同的合同措施；

◆数据处理者应在充分考虑数据处理活动性质的基础上，在可能的情形下，通过采取适当的技术和组织措施协助数据控制者履行其在GDPR项下的义务，尤其是响应个人数据主体权利请求的义务；

◆数据处理者应根据数据控制者的选择，在所提供的数据处理服务结束后，及时删除或返还所处理的个人数据。除非欧盟或成员国法律另有关于个人数据存储的要求，还应当及时删除个人数据的备份或副本；

◆数据处理者应当向数据控制者提供能够证明其遵循GDPR合规要求的证明信息，并积极配合由数据控制者或其指定的审计机构/审计人员所进行的审计或核查活动。

数据控制者及数据处理者之间的合同应当以书面或电子的方式签署。

PART 07

如何进行数据跨境传输

向欧盟/欧洲经济区以外的国家或地区传输个人数据，不论是个人数据在物理上跨越国境发生转移的情形还是个人数据被远程访问的情形，均属于GDPR项下的个人数据跨境传输，均需具备相应的传输保障机制[1]。一般来说，企业所适用的传输保障机制主要包括以下三项：

7.1 充分性决定

当欧盟委员会作出充分认定认为某一国家、地区、行业或国际组织能够确保充分的保护水平时，个人数据可以向此类国家或地区传输且不需要特别授权。目前，充分性认定的国家或地区包括：安道尔；阿根廷；加拿大(商业组织)；法罗群岛；根西岛；以色列；马恩岛；泽西岛；新西兰；瑞士；乌拉圭；美国（仅限于隐私盾保护框架）；日本[2]。

1.根据GDPR第49条，以及EDPB于2018年5月25日发布的Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679，在以下特殊情形下若无适当的跨境传输保障机制仍可进行传输：(a)数据主体已充分知悉潜在风险，且明确同意传输；(b)为履行数据主体与控制者之间的合同，或应数据主体的请求所采取的合同签订前的事先措施所必要的传输；(c)传输对于控制者履行与第三方的合同是必要的，且该合同履行有利于保护数据主体的利益；(d)传输对于公共利益目的是必要的的；(e) 出于建立、行使或抗辩法律目的；(f)当数据主体客观上或法律上不能作出同意时，为了保护数据主体或他人的重要利益进行传输是必要的；(g)根据欧盟或欧盟成员国法律，传输是由相应机构进行的，且该机构向公众提供咨询，但仅在符合特定的欧盟或欧盟成员国的特殊规定时才能进行。

2.https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

7.2 具有约束力的公司规则（Binding Corporate Rules, BCRs）

具有约束力的公司规则适用于集团内部之间个人数据的传输，须经监管机构批准。该规则具有法律约束力，由企业集团的成员及其员工所执行。具体约束力的公司规则应当至少明确以下内容：

◆所适用的具体成员名称及详细联系方式；

◆依据此规则所进行的数据跨境传输所涉及的个人数据的类型、个人数据主体的类型；个人数据处理活动的类型及目的等。

7.3 标准合同条款

签订个人数据跨境传输标准条款是目前企业所广泛采取的传输保障机制。欧盟委员会制定有适用于不同数据处理角色间的标准合同条款[3]，其中明确了数据传输方及数据接收方就个人数据跨境传输所享有的权利及所应承担的责任义务，在具体签订时还是应当补充数据传输双方的基本信息（包括名称、所在国家或地区、联系方式等）以及个人数据传输的基本信息（包括传输目的、涉及的个人数据主体的类型、个人数据的类型、数量、所采取的技术和安组织安全措施等）。

目前标准合同条款由欧盟委员会制定，欧盟各成员国数据保护监管机构也可能发布其他版本的合同条款，应当持续关注。

3.包括decision 2001/497/EC, decision 2004/915/EC（欧盟境内数据控制者与非欧盟境内数据控制者之间的传输）以及decision 2004/915/EC（欧盟境内数据控制者与非欧盟境内数据处理者之间的传输）。

PART 08

企业的GDPR应对之道

8.1 企业面临的GDPR合规风险

（1）GDPR违规后果

欧盟各成员国的数据保护监管机构有权持续监督成员国境内的GDPR合规情况，监管机构在履行其职责时会充分考虑到如下因素：

◆在数据处理活动涉及多个成员国时，几个国家的数据保护监管机构可能会同时负责；

◆为了避免数据控制者或处理者承担重复责任，各数据保护机构之间采取一致性机制，由此产生一个处罚决定；

◆在涉及个人数据跨境传输的情形下，需有一个代表的数据保护机构作为数据控制者或处理者的唯一联系人。

需要中国企业关注的是，对于在欧盟境内无经营场所但根据GDPR第3条适用于GDPR的数据控制者或数据处理者而言，在判断落入哪个国家数

据保护机构监管范围时可考虑如下因素：数据处理活动主要在哪个国家进行?受影响的个人数据主体主要位于哪个国家?以及哪个国家的数据保护机构已收到来自个人数据主体的投诉?

数据保护监管机构有权在GDPR规定的基础上，根据所在成员国的具体法律规定行使处罚权利。根据GDPR的规定，违反有关儿童同意、设计和默认的数据保护、共同数据控制者、代表设立、数据处理者、数据处理活动记录、监管机构配合、数据安全保障、数据泄露通知、数据保护影响评估及数据保护官的相关规定的，最高可处1千万欧元或相当于其上一年全球总营业额2%的金额的罚款，两者取其高的一项进行罚款。如果违反的是有关数据处理活动的基本原则及法律基础、数据主体的权利、个人数据跨境传输相关规定、成员国的法律规定以及监管机构的命令的，最高可处2千万欧元或相当于其上一年全球总营业额4%的金额的罚款，两者取其高的一项进行罚款。

(2) GDPR适用风险

对于中国企业而言，判断是否适用于GDPR、明确受GDPR约束的业务范围是开展合规工作的第一步。GDPR不仅适用在欧洲设立的机构，而且还会波及将欧盟客户作为业务目标的企业。对于后者，具体而言，包括为欧盟内的数据主体提供商品或服务（不论是否收费），以及对欧洲范围内的数据主体的活动进行监控（monitor）。

基于上述规定，在欧盟境内设立有代表处、分支机构等的中国企业需判断所设立的机构或人员是否因开展实际有效的业务活动而构成营业场所；在欧盟境内无任何机构的中国企业则需判断是否向欧盟境内的个人数据主体提供产品或服务，或者构成对个人数据主体活动的监控。其中，监控包括多种形式，例如使用cookies或其他跟踪技术进行在线跟踪、基于用户画像进行市场调查等。

(3) GDPR合规风险

如前所述，若违反GDPR的合规要求可能导致高额的处罚。在GDPR项下，当数据控制者或者处理者违反相关规定，未遵守数据处理的基本原则和法律基础的规定，对数据主体的权利造成损害时，数据主体有权直接向监管机构进行投诉，监管机构可决定向其提供司法救济渠道，以及是否对违规主体进行行政处罚。

除受到监管机构的处罚以外，违规事件对于企业的商业利益、商誉等均会造成较大的影响。至于企业可能面临的风险等级，企业可以结合自身欧盟市场的具体情况进行评估，总体而言：

◆对于大企业、处理大量数据的企业，其合规要求较高，其面临法律风险

的几率也会增大。欧盟在制定GDPR过程中，也充分考虑了大企业和中小型企业（SMEs）的不同情况，大企业承担高标准责任是一个共识；

◆如果企业遭受数据主体的投诉，也会增加企业面临的法律风险，数据监管机构的调查可能会因为对数据主体的调查而展开；

◆企业如果面临数据泄露的风险或发生了数据泄露，可能会导致数据监管机构的调查。

（4）英国脱欧对中国企业的影响

2020年1月31日，英国正式脱离欧盟，进入一年的脱欧过渡期。在过渡期期间，英国与欧盟需达成新的自由贸易协定。因此，实际上在过渡期内的英国仍需执行欧盟的各项规则。英国信息保护委员会（Information Commissioner's Office，"**ICO**"）发布的关于英国脱欧相关问题解答（Information rights and Brexit Frequently Asked Questions）中表明，签署脱欧协议后至2020年年底为过渡期，在此期间英国仍正常适用GDPR。过渡期结束后，英国可能不再适用GDPR，但英国境内企业均需遵守英国数据保护法案（Data Protection Act 2018），根据GDPR第3条适用GDPR的企业仍须遵守GDPR的各项规定。

因此，对于面向英国境内数据主体提供产品及服务的中国企业而言，针对英国境内个人数据主体所进行的数据处理活动短期之内仍需满足GDPR的要求。同时，企业应当持续关注英国与欧盟协议签署的推进情况，及时进行相应调整。

8.2 企业实现GDPR合规的路径

GDPR合规是企业系统性整改的过程，涉及不同的职能部门，包括全部受影响的产品，最后落实到具有实施力的企业组织措施和技术措施上。我们认为，在GDPR合规中，应当覆盖四个要素，合规过程分为三个阶段。

四个要素即组织、流程、规章和培训，构成了一个完整的企业数据保护体系建设（Data Protection Management，DPM）。GDPR绝非一个法律部门或IT部门就能完成的工作，其首先需要的是管理层的重视，由管理层下达企业的决策，对执行合规的部门（核心包括法律和IT）进行必要的授权，安排充分的人力和财力资源，这是启动合规项目的第一步；GDPR所规范的数据处理活动包括数据的整个生命周期，GDPR合规中也需要进行全流程、全生命周期的合规，要根据数据的Data Mapping定位数据流，进而确定风险点和合规点。数据的流转既包括在组织内部的流转，也包括在组织外的流转，比如数据处理、共享和跨境的传输等；GDPR的合规核心是企业的组织措施和

技术措施，保证这些措施的效力和可执行性，需要通过企业的规章制度和标准程序来实施，这些完成的规章制度和标准流程必须是针对企业现状的、并实时更新的；制度和合规培训是企业执行GDPR合规项目必要的阶段，其可以让相关的部门和员工了解其所承担的责任及要求，保证实施的效果，也可以培养企业数据保护的意识。

GDPR的合规过程一般分为三个阶段，即：差距分析，风险分析及合规建议，合规方案的实施和优化。

（1）第一步：差距分析

为评估一个企业的数据保护状况，首先必须要分析数据保护合规的现状与GDPR所规定的义务之间的差距。这需要收集企业数据保护合规现状的相关信息，例如：处理数据的部门、处理数据的目的、处理的数据类型、内部责任的划分、数据主体权利的保障措施、数据保护官制度的实施、IT安全措施等；其次，评估特定适用于一个企业的GDPR要求。

（2）第二步：风险分析及合规建议

实现GDPR的要求并非易事，同时合理地满足所有的需求有相当难度。企业需评估各项数据处理活动对企业业务、数据主体的权利以及导致法律风险的可能性等的风险程度，合理调配资源，提出可行的合规建议。

（3）合规方案的实施和优化

GDPR的实现过程需要其所涉及的企业欧洲实体的配合，以及企业管理层对于合规事务的明确认知。如果在欧盟设有办事处或实体，企业应将项目职责分配给相关企业欧盟办事处的关键人员，并指定一名主管项目经理领导该项目。若没有办事处或实体，可考虑先从设立GDPR规定的代表开始，结合其他合规措施一起推进。

PART 09

GDPR执法案例风险映射

GDPR自2018年5月25日生效以来，欧盟各国数据保护机构不断加强执法频率及力度。欧盟数据保护委员会（European Data Protection Board, EDPB）于2019年5月22日发布的GDPR实施一周年报告中的数据[4]显示，截至2019 年3 月，共上报281,088例案件。案件主要分为3个主要类别，其中近半数（144,376件）是投诉，近三分之一（89,271件）是数据泄露，其余（47,441件）涉及其他问题。2019年下半年以来，出现了以英国航空公司（因数据泄露被处以2.04亿欧元的罚款）及某酒店集团（因数据泄露被处以1.1

4.https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en 访问时间：2019年12月28日

亿欧元的罚款）为代表的天价罚款案例，同时执法数量也在持续增加。

为紧贴GDPR执法和监管态势，明确执法机构所关注的痛点问题，我们选取了部分典型执法案例，对其中的基本场景事实进行梳理提炼，针对不同的实践场景进行风险提示。本指引将提炼出的事实分为三类：

①日常活动，即企业员工在日常工作当中不可避免的各类活动；

②业务拓展活动，即在开展业务时可能会涉及到的应用投放、广告发送等活动；

③员工管理活动，即企业内部对员工进行管理时可能涉及个人数据处理的各项活动。

企业可参照以下风险提示对所进行的各项数据处理活动进行自评与审查，采取相应的措施防控合规风险。

9.1 日常活动

针对日常中的各项活动，企业应当指导员工准确判断是否会涉及对个人数据进行处理、明确进行数据处理活动所应遵守的各项要求，尽量避免员工在日常活动中可能出现的各类不合规行为。

序号	具体场景		风险提示（处罚要点）	代表案例
1	文档签名	采用电子形式签署协议，收集个人数据主体的生物特征签名数据。	根据GDPR第5条目的限制原则及数据最小化原则的要求，个人数据的收集和处理应当严格限制在实现特定目的所必要的最小范围内。在本场景下，实质上通过签署纸质版协议也可以实现同样的目的，无需使用电子协议的形式。	所在国家：捷克 监管机构：Úřad pro ochranu osobních údajů（the Office for Personal Data Protection, UOOU） 处罚对象所属行业：金融机构 罚款数额：9,704欧元
2	网络发布	新闻媒体在以电子及纸质报纸形式对非法拘留案件进行报道时，披露警员的姓名和照片。	根据GDPR第5条目的限制及数据最小化原则以及第6条关于数据处理活动法律基础的要求，在本场景下，仅通过提及数据主体姓名的首字母或通过面部模糊、远距离拍摄等方即可实现新闻报道的目标，且上述方式不会对	所在国家：塞浦路斯 监管机构：Office of the Commissioner for Personal Data Protection 处罚对象所属行业：新闻媒体 罚款数额：10,000欧元

序号	具体场景		风险提示（处罚要点）	代表案例
			新闻报道中的事件带来实质影响，直接披露警员的姓名不具备相应的法律基础，超出了一般新闻媒体报道所必要的范围。	
3	邮件收发	某个人采用抄送而非密送方式向多人发送电子邮件，导致每个人可以看到其他人的个人邮箱地址，后被指控涉及多起侵权行为。	根据GDPR第6条，数据处理活动均应具备适当的法律基础。在本场景下，向第三方披露数据主体的邮箱地址不具备相应的法律基础。	所在国家：德国 监管机构：The Federal Commissioner for Data Protection and Freedom of Information (BfDI) 处罚对象所属行业：个人 罚款数额：2,000欧元
4	纸质文件	纸质文件被保存在没有任何防护措施的纸箱中，导致其中包含的个人数据泄露。	根据GDPR第5条完整性、保密性原则以及GDPR第32条关于个人数据安全的要求，在本场景下，对于纸质文件的保存未采取适当的防护措施，导致了其中个人数据的意外丢失。	所在国家：捷克 监管机构：Úřad pro ochranu osobních údajů (the Office for Personal Data Protection, UOOU) 处罚对象所属行业：金融机构 罚款数额：1,165欧元
5	便携存储	某数据控制者丢失了包含有个人数据的闪存驱动器，造成个人数据泄露，且未在72小时内及时通知监管机构。	根据GDPR第32条及第33条的规定，应当采取适当的组织和技术措施，确保个人数据的安全性和机密性，并应当在发生个人数据泄露事件后72小时内及时通知监管机构。在本场景下，未采取适当措施保证便携存储设备的安全，且未按照要求通知监管机构。	所在国家：匈牙利 监管机构：The National Authority for Data Protection and Freedom of Information（NAIH） 处罚对象所属行业：个人 罚款数额：15,150欧元

序号	具体场景		风险提示（处罚要点）	代表案例
6	视频监控	某商店在店前安装了视频监控设备，对店面前的人行道进行监控拍摄，且未明确标识监控区域。	根据GDPR第13条，收集处理个人数据时，应当向数据主体提供数据处理活动相关的信息。在本场景下，对公共区域进行监控，但未以明确标识等方式向可能涉及的数据主体告知监控范围及所进行的数据处理活动。	所在国家：奥地利 监管机构：Austrian Data Protection Authority 处罚对象所属行业：/ 罚款数额：4,800欧元
7	安保活动	为保证安全，某音乐节组织者要求观众提供国籍、姓名、性别、证件号码以及图像和声音的等数据，并均以数据主体的同意作为此项数据保护的法律基础。	一方面，根据GDPR第5条目的限制及数据最小化原则的要求，在本场景下，可以通过金属探测器或安全筛查等措施实现安保目的而无需过多地收集个人数据。 另一方面，根据GDPR第6条关于法律基础的要求，本场景下所进行的数据处理活动无需以数据主体的同意作为法律基础，且由于数据主体拒绝提供相关信息将导致其不能入场，同意存在瑕疵。	所在国家：匈牙利 监管机构：The National Authority for Data Protection and Freedom of Information（NAIH） 处罚对象所属行业：文化娱乐 罚款数额：92,146欧元
8	权利响应	数据主体要求删除数据控制者删除其个人数据，其该请求已得到控制者确认，但后来数据主体又连续收到控制者的相关信息，原因是控制者未实际删除且错误地将该数据主体的个人数据用于测试。	根据GDPR第17条，数据主体享有被遗忘权，即有权要求删除其个人数据，数据控制者及处理者应当采取相应措施确保数据主体权利请求的实现。在本场景下，数据控制者未充分响应数据主体要求删除其数据的权利请求，违反了GDPR的规定。	所在国家：西班牙 监管机构：Agencia Española de Protección de Datos (AEPD) 处罚对象所属行业：电信通讯 罚款数额：27,000欧元

9.2 业务拓展活动

业务拓展活动是企业最主要从事、因此最为关注的一类活动。企业在进行具体业务活动时，应当结合业务具体情况，从源头把控风险，采取各项适当的组织措施和技术措施，确保数据处理活动合规进行，数据主体权利得到充分保障。

序号	具体场景		风险提示（处罚要点）	代表案例
1	广告发送	在未经数据主体授权的情况下即向发送电子邮件广告。此外，在数据主体明确反对将其个人数据用于广告投放后，仍然收到电子邮件广告。	根据GDPR第21条，当因为直接营销目的而处理个人数据，数据主体有权随时反对此类处理活动。在本场景下，数据控制者未充分响应数据主体反对将其个人数据用于广告投放的权利请求，仍向其发送营销广告，违反了GDPR的规定。	所在国家：德国 监管机构：The Federal Commissioner for Data Protection and Freedom of Information (BfDI) 处罚对象所属行业：外卖平台 罚款数额：195,407欧元
2	公开渠道获取	从公开渠道获得个人数据用于商业目的，以高额运营成本为由未向数据主体提供相关信息。	根据GDPR第14条，在不是从数据主体处直接收集个人数据时，同样需向数据主体提供数据处理活动的相关信息以满足透明性的要求。	所在国家：波兰 监管机构：Urząd Ochrony Danych Osobowych (Personal Data Protection Office, UODO) 处罚对象所属行业：互联网（数字营销） 罚款数额：219,538欧元 (*最终罚款数额正在重新审定中)
3	供应商管理	某数据控制者因服务提供商拒绝前签署数据处理协议而未与其签署，但仍委托该服务提供商处理数据。	根据GDPR第28条的规定，数据处理者的处理行为应当受到合同或相关法律规定的约束。在本场景下，数据控制者指定第三方供应商处理客户数据，未签署数据处理协议，在不知道供应商数据处理流程的情况还将数据传送给其进行处理，违反了GDPR的规定。	所在国家：德国 监管机构：The Federal Commissioner for Data Protection and Freedom of Information (BfDI) 处罚对象所属行业：互联网 罚款数额：5,000欧元

序号	具体场景		风险提示（处罚要点）	代表案例
4	收购投资	在收购时未发现收购对象的数据系统安全系统漏洞，造成严重的个人数据泄露。	根据GDPR第32条，应当采取适当的组织和技术措施保障个人数据安全，避免个人数据非法销毁、丢失、篡改、未经授权的披露或访问。在本场景下，在收购投资时未进行充分的尽职调查发现存在的系统漏洞，同时缺乏保障数据安全的技术和组织措施。	所在国家：英国 监管机构：Information Commissioner's Officer (ICO) 处罚对象所属行业：酒店 罚款数额：1.1亿欧元
5	应用投放	在应用投放前未经过适当的测试，存在重大安全漏洞，导致数据泄露。	根据GDPR第32条，应当采取适当的组织和技术措施保障个人数据安全。在本场景下，在应用投放市场前未进行充分的安全测试，未及时发现产品存在的安全漏洞，违反了GDPR的规定。	所在国家：挪威 监管机构：The Norwegian Data Protection Authority 处罚对象所属行业：行政机关 罚款数额：203,000欧元

9.3 员工管理活动

针对员工管理过程中发生的个人数据处理活动，在论证数据处理活动所依据的法律基础、对员工个人数据进行处理时均应充分考虑公司与员工之间关系的特殊性，避免因双方之间的不平等导致所采取的措施不适当。

序号	具体场景		风险提示（处罚要点）	代表案例
1	员工管理	在针对员工的个人数据进行处理时，以数据主体的同意作为数据处理活动所依据的法律基础。	根据GDPR第6条，数据处理活动应当具备适当的法律基础。由于公司和员工之间关系的不平等，此类同意不能认定为是基于员工自由意志作出的，不构成满足GDPR要求的有效同意。	所在国家：希腊 监管机构：The Hellenic Data Protection Authority 处罚对象所属行业：咨询 罚款数额：150,000欧元

序号	具体场景		风险提示（处罚要点）	代表案例
2	信息公示	在公开网络上披露内部人员的相关信息时，超出必要的范围，导致可能存在未经授权使用所披露的个人数据的风险。	根据GDPR第5条目的限制及数据最小化原则的要求，对个人数据的使用应当严格仅限于实现目的所需要的最下必要范围内。在本场景下，如确有必要公开披露员工信息的，超出了最小必要的范围。	所在国家：波兰 监管机构：Urząd Ochrony Danych Osobowych (Personal Data Protection Office, UODO) 处罚对象所属行业：体育 罚款数额：12,950欧元
3	视频监控	公司出于确保人员和财产安全的目的安装视频监控设备，对员工进行持续的监控。	一方面，根据GDPR第5条目的限制及数据最小化原则的要求，在本场景下，可以通过调整监控设备的安装位置、方向、操作周期等进行持续永久的监控。 另一方面，根据GDPR第6条关于法律基础的要求，在工作场所安装视频监控设备需具备具体、明确的目的，并需具备适当的法律基础。	所在国家：法国 监管机构：The Commission nationale de l'informatique et des libertés (CNIL) 处罚对象所属行业：未知 罚款数额：20,000欧元
4	人脸识别	将人脸识别技术用于考勤，以数据主体的同意作为该项数据处理活动作为法律基础，同时在将人脸识别投入使用前没有进行数据保护影响评估，未与数据保护机构进行沟通。	一方面，根据GDPR第6条关于法律基础的要求，由于公司和员工之间关系的不平等，此类同意不能认定为是基于员工自由意志作出的，不构成满足GDPR要求的有效同意。 另一方面，根据GDPR第35条的规定，在特定情形下需进行数据保护影响评估，并积极与数据保护机构进行沟通。	所在国家：瑞典 监管机构：The Swedish Data Protection Authority 处罚对象所属行业：教育 罚款数额：18,630欧元

结合上述典型案例的事实提炼及风险映射分析，为积极应对数据主体的投诉及监管机构的审查，企业内部应当依据法律要求及行业实践明确合规要求、制定合规规范、嵌入业务流程，其中重点建议关注以下问题：加强个人数据安全保障，避免发生个人数据非法访问、使用及意外泄露、毁损、灭失等请求；重视数据主体权利请求，做到积极响应、切实实现，减少数据主体投诉；在开展新业务、新活动时进行充分的风险评估，及时采取风险应对措施；加强员工培训，提升整体合规意识水平。

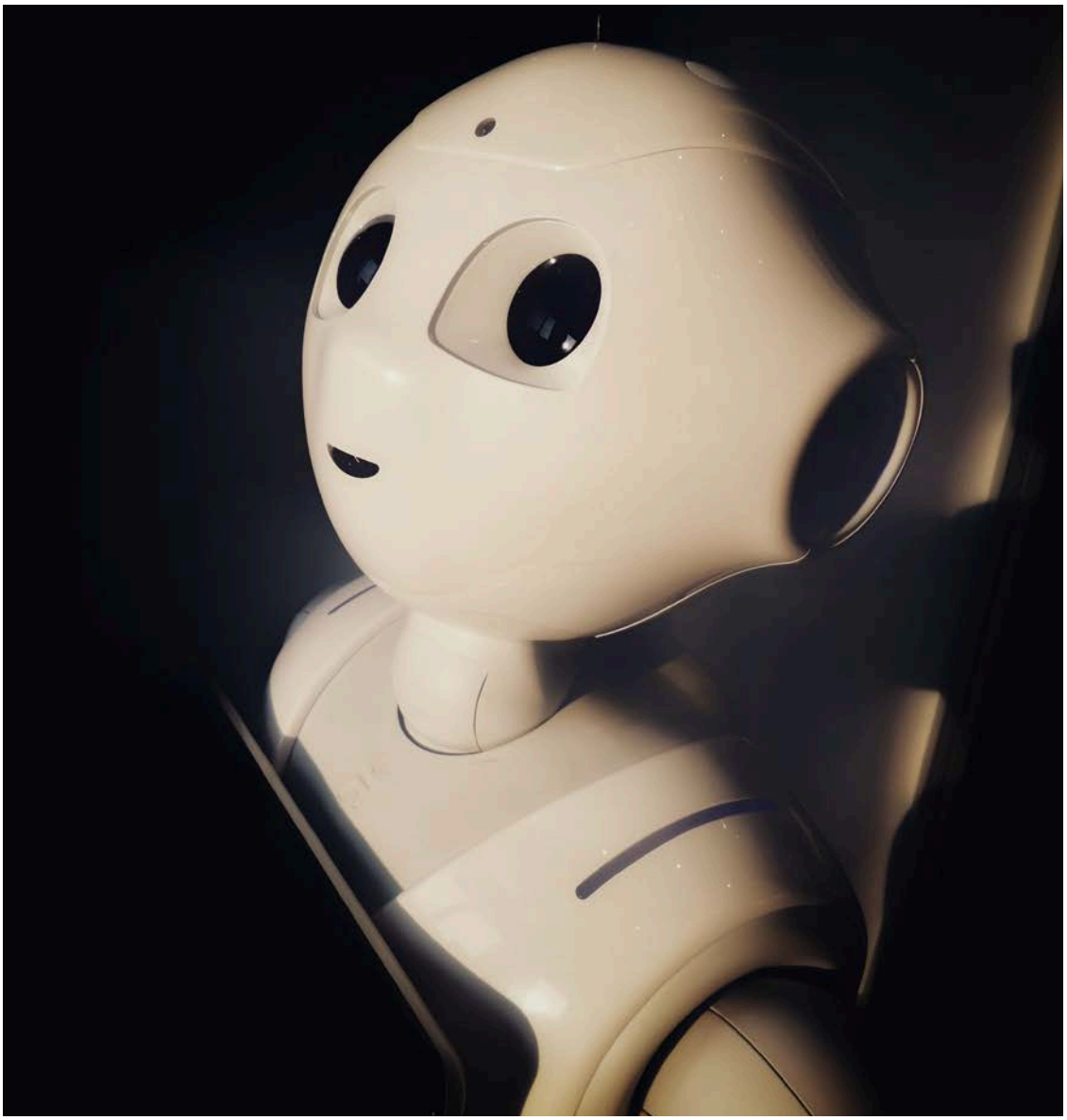
陈际红
合伙人
知识产权部
北京办公室
+86 10 5957 2003
chenjihong@zhonglun.com

CHAPTER

3

人工智能技术的应用、资本市场与监管

APPLICATION,
CAPITAL MARKET AND
REGULATION OF ARTIFICIAL INTELLIGENCE



人工智能在互联网医疗领域的应用和合规风险分析

作者/傅长煜、左玉茹、韩越

早在2017年，国务院就已发布《新一代人工智能发展规划》（国发〔2017〕35号），提出“推广应用人工智能治疗新模式新手段，建立快速精准的智能医疗体系。探索智慧医院建设，开发人机协同的手术机器人、智能诊疗助手，研发柔性可穿戴、生物兼容的生理监测系统，研发人机协同临床智能诊疗方案，实现智能影像识别、病理分型和智能多学科会诊。基于人工智能开展大规模基因组识别、蛋白组学、代谢组学等研究和新药研发，推进医药监管智能化。加强流行病智能监测和防控。”国发〔2017〕35号所探索的人工智能在医疗领域的应用场景较为广泛，覆盖了医院管理、辅助诊疗、可穿戴设备、影像分析等。近年来，随着人工智能技术的优化和互联网医院的发展，人工智能技术在互联网诊疗中的应用逐渐铺开，应用场景从最初的智能分诊导诊，逐步发展出智能问诊、智能处方审核、智能医疗数据管理、智能诊后管理等整个诊疗流程的各个方面，人工智能技术在提高互联网医院的工作效率方面的确起到了非常重要的作用，但同时，对于诊疗安全和诊疗质量也带来了新的问题。近年来，有不少规则政策出台尝试规范人工智能技术在医疗领域的应用，比如近期发布的《人工智能医用软件产品分类界定指导原则》。本文旨在梳理人工智能技术在互联网医疗中的应用现状，结合相关规则，分析应用过程中的合规风险。

PART 01

互联网诊疗流程概述

互联网诊疗一般流程包括：(1) 导诊及分诊 (2) 接诊 (3) 开具处方 (4) 诊后管理。

(一) 导诊与分诊

患者进入到互联网医院界面后，如有诊疗服务需求，需要先通过一个导诊环节。互联网医院会先行收集患者病情信息，包括病情症状、患者信息、病历资料等。在收集上述信息后，再根据收集的信息提供科室类别建议，患者可确认是否进入所建议科室进行问诊。

(二) 接诊

导诊、分诊到具体科室、具体医生后，便正式开始线上问诊环节。现行规定对互联网诊疗的主要要求包括：

1. 诊疗服务的范围

医生仅能通过互联网开展部分常见病、慢性病复诊，不得通过互联网开展首诊活动。医师应当掌握患者病历资料，确定患者在实体医疗机构明确诊断为某种或某几种常见病、慢性病后，可以针对相同诊断进行复诊。

一些地方性规范则对如何落实首诊禁止规则提出了更具体的要求，例如，《上海市互联网医院管理办法》进一步要求患者需要提供2个月内的病历资料，医生应充分掌握患者既往病史、诊断和处方用药情况。《海南省互联网医院管理办法（试行）》提出应至少符合以下条件之一：（1）患者可以提供在实体医疗机构既往就诊病历的电子文档；（2）患者可以提供在其他互联网医院就诊的电子病历；（3）互联网医院经患者授权通过人口健康信息平台或第三方平台获取患者电子健康档案；（4）互联网医院经患者授权通过实体医疗机构获取患者电子病历；（5）患者在执业医师陪同下在互联网医院就诊。

2. 患者知情同意

互联网医院必须事先对患者进行风险提示，获得患者的知情同意。

3. 互联网诊疗服务终止

当患者出现病情变化需要医务人员亲自诊查时，医疗机构及其医务人员应当立即终止互联网诊疗活动，引导患者到实体医疗机构就诊。

（三）处方开具、审核

互联网医院的医师、药师应当根据《执业医师法》、《医疗机构处方审核规范》、《处方管理办法》等相关法律法规的要求，书写、开具、审核处方。

在处方开具方面，只有取得了互联网医院处方权的医师才能开具处方，医生在掌握患者病历资料后，可以为部分常见病、慢性病患者在线开具处方，但不得开具麻醉药品、精神药品等特殊管理药品的处方。为低龄儿童（6岁以下）开具互联网儿童用药处方时，应当确认患儿有监护人和相关专业医师陪伴。

在处方审核方面，互联网医院需配备专职药师负责在线处方审核工作，确保业务时间至少有1名药师在岗审核处方。药师人力资源不足时，可通过合作方式，由具备资格的第三方机构药师进行处方审核。

（四）诊后管理

线上诊疗结束并不意味着医疗服务的结束，诊疗、用药后的患者身体症状变化、治疗效果等都需要持续关注，特别是对于慢性病管理、老年人诊疗，更需要长期随访、提供诊后医疗服务。互联网诊后管理的内容主要包括诊后随访、慢病管理等。

PART 02

人工智能在互联网诊疗流程中的具体应用

(一)智能分诊、导诊

在导诊环节,面对互联网医院庞大的问诊量,互联网医院多会设置人工智能来进行分诊、导诊,由人工智能与患者“对话”的方式,收集患者病情信息。

在收集上述信息后,人工智能运用大数据分析,根据收集的信息提供科室类别建议。如果人工智能无法判断具体科室的,如医院有配备全科科室,则可以分诊到全科科室,再由全科科室的医师视情况确定是否再需分到其他科室还是直接建议线下诊断。

图1. 智能导诊系统示例[1]

1.图片来源:https://open.-zuoshouy-isheng.com/product?-type=dz&zy_chan-nels=baidupc&bd_vid=10536594813428357608

(二)智能问诊

诸多互联网医院在问诊环节接入了人工智能问诊技术。人工智能问诊技术又根据问诊输出结果不同区分为“预问诊”、“辅助诊疗”和“问诊开方”等几种类型。

1. 预问诊系统

“预问诊”是指在正式接诊前,由人工智能与患者之间进行互动,收集问诊所需的全部信息,形成病历档案,该过程的输出结果是患者的病历档案,不涉及对患者病历信息的分析处理,而只是将收集形成的病历信息传递至接诊医生,为医生接诊前期病历信息搜集的时间,医生可根据人工智能搜集的结果进行诊疗活动。

2.图片来源：https://open.zuoshouyisheng.com/product?type=yw

图2. 智能预问诊系统示例[2]

2、辅助诊疗系统

人工智能的辅助诊断目前主要应用于临床医学影像解读、诊断提示等领域，深度学习的人工智能，在对图像的检测效率和精度两个方面，正确率可能比人还要高，运用人工智能进行辅助诊断，能够减少主观因素带来的误判，提高诊断速度，也有利于尽早发现疾病隐患。

2020年，我国有10款人工智能医疗器械产品获批上市，如北京昆仑医云科技有限公司生产的创新产品“冠脉血流储备分数计算软件”、乐普医疗的人工智能“心电分析软件”、安德医智的颅内肿瘤磁共振影像辅助诊断软件、上海鹰瞳医疗科技有限公司生产的创新产品“糖尿病视网膜病变眼底图像辅助诊断软件”等。

3、综合诊疗系统

“问诊开方”系统则并不止步于收集患者信息，基于收集的患者信息，具有“开方”功能的问诊系统将对患者主诉进行分析、作出诊断结论、开具处方。比如“发明专利-基于证素和深度学习的中医智能问诊舌诊综合系统”，“本发明提供了一种基于证素和深度学习的中医智能问诊舌诊综合系统，基于症状的证素，根据预设知识图谱，分析患者输入的症状信息；基于症状分析的结果，判定是否需要进行问诊；若判定结果为需要进行问诊，则利用证素和深度学习网络模型进行中医问诊，根据患者的回答，得到患者的证候和

/或证素；判定是否结合舌诊，如是，则问诊模块的结果进入结合舌诊模块，得到最终证候和/或证素；否则，以问诊得到的结果为最终证候和/或证素；当问诊判定模块判定不需要进行问诊或者舌诊判定模块判断需要结合舌诊时，基于证素和深度学习网络模型，综合患者的症状和舌象信息，得到最终证候和/或证素；能够大大提高问诊的效果，为辨证分型提供了强有力支撑。”

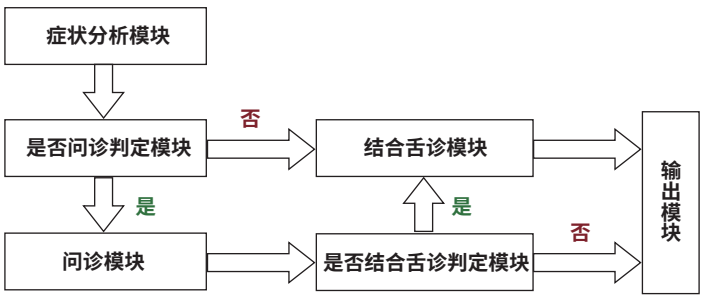


图3. 发明专利基于证素和深度学习的中医智能问诊舌诊综合系统的摘要及附图[3]

3.图片来源于国家知识产权局官方网站专利检索系统，专利申请号：CN202011155816.3，系该发明专利的摘要附图

4、辅助开方系统

部分互联网医院在开方环节也接入了人工智能技术，直接通过系统开具初步处方，然后由医师审核确认处方。但目前辅助开方系统的应用并不是十分普遍。

（三）智能审方系统

在一般诊疗流程中，处方开具之后，进入药师审方环节。在互联网医院中，处方审核接入人工智能技术已较为成熟，目前已有不少审方技术申请专利权，比如：某发明：一种医疗处方审核系统及方法。一种医疗处方审核系统及方法，“本发明公开了一种医疗处方审核系统及方法，涉及医疗技术领域，包括：第一数据库，预存有标准处方信息；第二数据库，预存有历史就诊信息；存储模块，用于存储医生上传的处方信息；审核模块，用于审核处方信息是否合规；处理模块，用于将最终处方输出至一配送模块，所述配送模块进行药品的调配。本发明的技术方案的有益效果在于：顺应了政策的要求，改造了现有的电子处方流转途径，创造性的建设了用药决策知识库，解决了原有人工审核时效率低下的弊端，提升了对处方合理性的审核效果，实现了均一性的审核标准，实现了互联网医院、社会药店处方外配以及医联体内的处方审核，并可开展后续处方点评工作，对用药决策知识库的规则进行维护。”[4]

4.检索自国家知识产权局官方网站专利检索系统，专利申请号：CN202011272858.5

5.图片来源于国家知识产权局官方网站专利检索系统，专利申请号：CN202011272858.5，系该发明专利的摘要附图

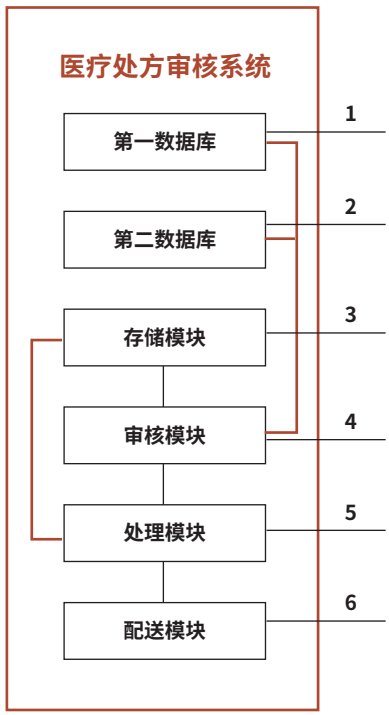


图4. 发明专利：一种医疗处方审核系统及方法的摘要附图[5]

（四）诊后管理系统

人工智能可以记录、存储患者问诊购药的过程，并结合大数据技术对患者的就诊记录进行分析，协助医生对患者制定精准化的随访计划，对随访结果进行智能分析。例如，评估病情恢复进展、预测病情复发概率、记录处方及用药变更信息、对病情进行智能追踪等，可以为医生提供患者更多、更准确的就诊后病情信息，为慢病治疗提供依据。

PART 03
关于人工智能在互联网医疗领域应用的政策法规

（一）关于人工智能在医疗领域应用的规范性文件

2018年4月25日，国务院办公厅发布《国务院办公厅关于促进“互联网+医疗健康”发展的意见》（国办发〔2018〕26号），在医疗机构建设层面，“鼓励医疗联合体内上级医疗机构借助人工智能等技术手段，面向基层提供远程会诊、远程心电诊断、远程影像诊断等服务，促进医疗联合体内医疗机构间

检查检验结果实时查阅、互认共享。推进远程医疗服务覆盖全国所有医疗联合体和县级医院，并逐步向社区卫生服务机构、乡镇卫生院和村卫生室延伸，提升基层医疗服务能力和效率”；在人工智能应用层面，“研发基于人工智能的临床诊疗决策支持系统，开展智能医学影像识别、病理分型和多学科会诊以及多种医疗健康场景下的智能语音技术应用，提高医疗服务效率。支持中医辨证论治智能辅助系统应用，提升基层中医诊疗服务能力。开展基于人工智能技术、医疗健康智能设备的移动医疗示范，实现个人健康实时监测与评估、疾病预警、慢病筛查、主动干预。加强临床、科研数据整合共享和应用，支持研发医疗健康相关的人工智能技术、医用机器人、大型医疗设备、应急救援医疗设备、生物三维打印技术和可穿戴设备等。顺应工业互联网创新发展趋势，提升医疗健康设备的数字化、智能化制造水平，促进产业升级。”

2018年7月17日，国家卫健委及中医药管理局发布《互联网诊疗管理办法（试行）》等3个文件，互联网医院建设、互联网诊疗正式开启规范化发展。不过，三部管理办法对于人工智能技术在互联网诊疗中的应用并没有提出明确要求。

2018年8月22日，国家卫健委发布《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》，提出：“通过电子病历信息化建设，探索建立健全智慧医院标准、管理规范和质量控制方式方法，发挥互联网、大数据、云存储、云计算、区块链、机器人等有关技术在医疗管理工作中的优势，逐步使患者在就诊过程中享受到更智能、更高效、更便捷、更安全、更富有人性化的个体化诊疗。鼓励将成熟的人工智能嵌入电子病历信息系统，发挥其在智能分诊导诊，辅助信息采集，辅助检验、病理、影像诊断，辅助诊疗决策支持，智能跟踪随访等方面的作用，提高医务人员工作效率，保障医疗质量与安全。”

2020年9月27日，国家卫健委及中医药管理局发布《关于加强全民健康信息标准化体系建设的意见》（国卫办规划发〔2020〕14），提出“3.推动医疗健康人工智能应用标准化建设。研究制订医学人工智能应用研究指南，推进医学人工智能在智能临床辅助诊疗、医用机器人、人工智能药物研发、智能公共卫生服务、智能医院管理、智能医疗设备管理、智能医学教育等领域应用试点和示范。加快研究制订人工智能技术的相关应用标准和安全标准，构建人工智能技术应用及安全测评标准，提升人工智能技术应用质量，强化人工智能技术应用安全管理。”

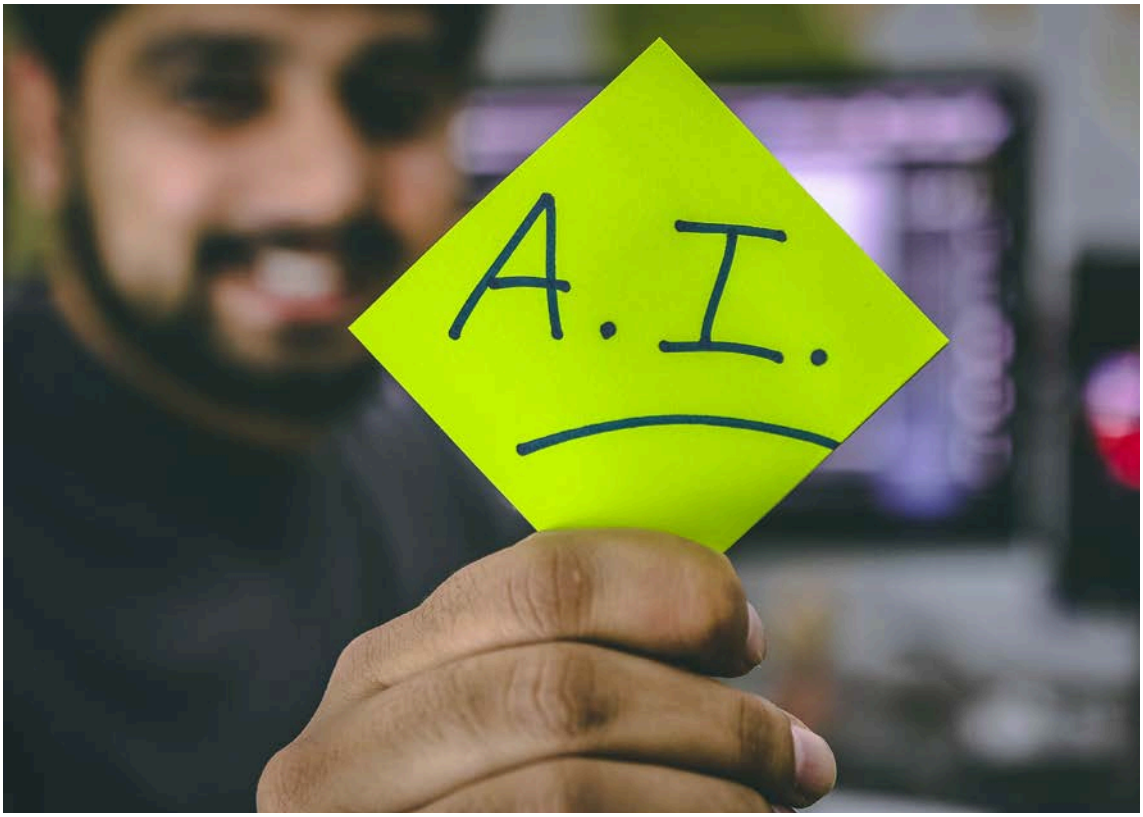
综上，人工智能技术在医疗领域的应用是受到政策鼓励支持的，支持发展的方向比较广泛，互联网医疗领域即属于重点发展方向之一。

（二）关于人工智能在医疗器械应用中的审评规范

2019年7月3日，国家药监局、医疗器械技术审评中心发布《深度学习辅助决策医疗器械软件审评要点》，对基于医疗器械数据（医疗器械所生成的医学图像、医学数据，以下统称数据），使用深度学习技术进行辅助决策的软件提出具体审评要点要求。审评要点重点关注软件的数据质量控制、算法泛化能力、临床使用风险。其中，临床使用风险应当考虑数据质量控制、算法泛化能力的直接影响，以及算力所用计算资源（即运行环境）失效的间接影响。

2021年6月4日，为进一步规范人工智能医疗器械生存周期过程质控要求和注册申报资料要求，并统一审评要求，医疗器械技术审评中心基于《深度学习辅助决策医疗器械软件审评要点》，结合产品审评经验积累和监管科学研究成果，编写了《人工智能医疗器械注册审查指导原则（征求意见稿）》（**“指导原则”**），公开征求意见，截至目前该指导原则尚未正式发布。该指导原则将人工智能医疗器械界定为基于“医疗器械数据”，采用人工智能技术实现其预期用途的医疗器械。该指导原则对医疗器械数据具体界定为：医疗器械产生的客观医疗数据，如医学影像设备产生的医学图像数据（如X射线、CT、MRI、超声等图像）、医用电子设备产生的生理参数数据（如心电、脑电、血压、无创血糖等波形数据）、体外诊断设备产生的体外诊断数据（如病理图像、显微图像、有创血糖波形数据等）；通用设备产生的用于医疗用途的客观数据亦属于医疗器械数据，如数码相机拍摄的用于皮肤疾病诊断的皮肤照片、健康电子产品采集的用于心脏疾病预警的心电数据等。同时，对人工智能医疗器械进行了详细分类，介绍了人工智能医疗器械的生存周期过程、十五项技术考量、算法研究资料的要求、注册申报资料的要求等。

2021年7月1日，药监局出台《人工智能医用软件产品分类界定指导原则》（**“2021《指导原则》”**），对人工智能医用软件进行属性界定，提出“若软件产品的处理对象为医疗器械数据，且核心功能是对医疗器械数据的处理、测量、模型计算、分析等，并用于医疗用途的，符合《医疗器械监督管理条例》有关医疗器械定义，作为医疗器械管理。若软件产品的处理对象为非医疗器械数据（如患者主诉等信息、检验检查报告结论），或者其核心功能不是对医疗器械数据进行处理、测量、模型计算、分析，或者不用于医疗用途的，不作为医疗器械管理。” 对于医疗器械的具体分类，2021《指导原则》也给出了指导意见：“对于算法在医疗应用中成熟度低（指未上市或安全有效性尚未得到充分证实）的人工智能医用软件，若用于辅助决策，如提供病灶特征识别、病变性质判定、用药指导、治疗计划制定等临床诊疗建议，按照第三类医疗器械管理；若用于非辅助决策，如进行数据处理和测量等提供临床参考信



息，按照第二类医疗器械管理。”

截至目前，人工智能技术在医疗领域的应用所有标准化规定均鉴于人工智能医疗器械领域，产品属性界定、技术审核标准等问题已有不少规则可供参考。

PART 04

人工智能在互联网诊疗领域应用的合规风险分析

基于上文介绍的应用场景，人工智能在互联网诊疗领域的应用可以归纳为两个分支：(1)诊疗流程管理：智能分诊导诊，诊后智能随访；和(2)诊疗行为干预：智能问诊、智能审方。在诊疗流程管理层面，人工智能技术的接入优势十分明显，大大提高了诊疗效率，但在诊疗行为干预层面，人工智能技术的接入是否能够保障诊疗安全和诊疗质量则具有较高的不确定性，也正因为如此，在诊疗行为干预层面的人工智能技术应用，可能会面临较多的合规风险。

（一）诊疗行为干预型人工智能产品可能属于医疗器械，未经注册/备案而生产、销售、临床应用面临较高风险

根据《医疗器械监督管理条例》，医疗器械的界定标准主要是预期用途是否具有诊疗目的。我国医疗器械实行目录管理。《医疗器械分类目录》（“**《分类目录》**”）规定：“医疗信息管理软件属性界定原则，如果医疗信息管理软件仅仅是医院管理工具，管理内容是患者信息等非医疗诊断和/或治疗内容，不按照医疗器械管理。如果医疗信息管理软件包含患者诊断、治疗数据和影像，则按照软件处理对象（影像、数据）的不同，将软件产品规范到‘21-2影像处理软件’或者‘21-3数据处理软件’。”远程医疗会诊系统软件的属性界定规则亦然。

《分类目录》区分医疗器械与非医疗器械的关键因素是软件处理的数据是否包含患者诊断、治疗数据和影像，基于这一分类原则，智能问诊系统和智能审方系统应归属于医疗器械。比如“用中医证治的相关理论，使用数据统计等方法，实现各种征候的分析诊断和/或提供治疗建议”的“中医诊疗软件”即属于决策支持类软件，应归于II类医疗器械。

2021年7月1日，国家药监局发布《人工智能医用软件产品分类界定指导原则》（“**2021《指导原则》**”），规定：“若软件产品的处理对象为医疗器械数据，且核心功能是对医疗器械数据的处理、测量、模型计算、分析等，并用于医疗用途的，符合《医疗器械监督管理条例》有关医疗器械定义，作为医疗器械管理。若软件产品的处理对象为非医疗器械数据（如患者主诉等信息、检验检查报告结论），或者其核心功能不是对医疗器械数据进行处理、测量、模型计算、分析，或者不用于医疗用途的，不作为医疗器械管理。”

2021《指导原则》对分类规则进行了调整，将医疗器械界定为对医疗器械数据进行处理、测量、模型计算、分析的软件，并明确对于非医疗器械数据的梳理，如患者主诉信息、检验检查报告结论的软件不作为医疗器械管理。如根据该指导原则，分析处理患者提供的病情信息、医生观察的症状信息、检验检查报告结论信息的软件，不再属于医疗器械，这与《分类目录》的分类原则有明显的差异。

尽管2021《指导原则》限缩了医疗器械的范围，但《分类目录》截至目前仍未正式修改。在执法实践中，分类界定由各地药监部门具体进行，在执法惯性下，智能问诊系统、智能处方审核系统等附带医疗功能的智能系统被归于医疗器械的可能性仍然较大。一旦被归于医疗器械，产品上市即必须进行注册或备案，未经注册或备案而生产、经营、临床使用，均属于违法行为。

限缩医疗器械的范畴，产品无需经过漫长的临床试验和注册审批即可

进入市场，这对于人工智能技术在互联网医疗领域的应用与发展是利好，不过，这可能也会同时带来互联网诊疗安全和质量问题，因此，在应用人工智能技术时应注意合规边界。

（二）人工智能技术在问诊、开方和审方环节的应用应适度，不得替代医师、药师的职能

在整个诊疗流程中，有两个环节必须由医疗卫生专业人士完成：诊疗行为（包括问诊和处方开具）必须由医师完成，处方审核行为必须由药师完成。

1、互联网诊疗规范严禁以人工智能完全替代医师

2018年，国务院发布通知，鼓励将人工智能技术纳入电子病历系统，探索人工智能在诊疗与辅助诊疗中的应用。整体而言，人工智能技术在互联网诊疗中的应用是受到鼓励和支持的，但是，对人工智能技术的应用不能突破诊疗管理规范，诊疗开方必须由执业医师执行，人工智能技术不能替代执业医师的职能是前述管理规范的题中之义。

《银川市互联网诊疗服务规范（试行）》规定，不得用人工智能等技术完全代替医师进行问诊、书写病历、开具处方等诊疗行为。并且，《银川市互联网诊疗服务规范（试行）》还规定了互联网诊疗应遵循“线上线下一致”原则。诊疗服务中，只有医师通过互联网获取的信息和线下面诊获取的信息相同，并足以支撑作出和线下面诊相同的诊断和处置意见时，才能继续诊疗行为。即便有智能问诊系统收集患者病史、病症信息，进行初步分析，基于诊疗服务规范，医师仍需要与患者进行必要的交流，作出独立诊断意见、开具处方。医师完全依赖人工智能采集的信息出具诊断意见开具处方，是不能够满足诊疗服务规范的要求的。甚至，如没有医师与患者互动的信息留存，可能会被监管部门认为医师并没有真正参与诊疗行为，而仅仅是提供了签名而已。

2、处方管理规范严禁以人工智能替代药师

《互联网医院基本标准（试行）》规定：“互联网医院有专职药师负责在线处方审核工作，确保业务时间至少有1名药师在岗审核处方。药师人力资源不足时，可通过合作方式，由具备资格的第三方机构药师进行处方审核。”《医疗机构处方审核规范》第四条规定：“所有处方均应当经审核通过后方可进入划价收费和调配环节，未经审核通过的处方不得收费和调配。”第六条规定：“药师是处方审核工作的第一责任人。药师应当对处方各项内容进行逐一审核。医疗机构可以通过相关信息系统辅助药师开展处方审核。对信息系统筛选出的不合理处方及信息系统不能审核的部分，应当由药师进行人工审核。”

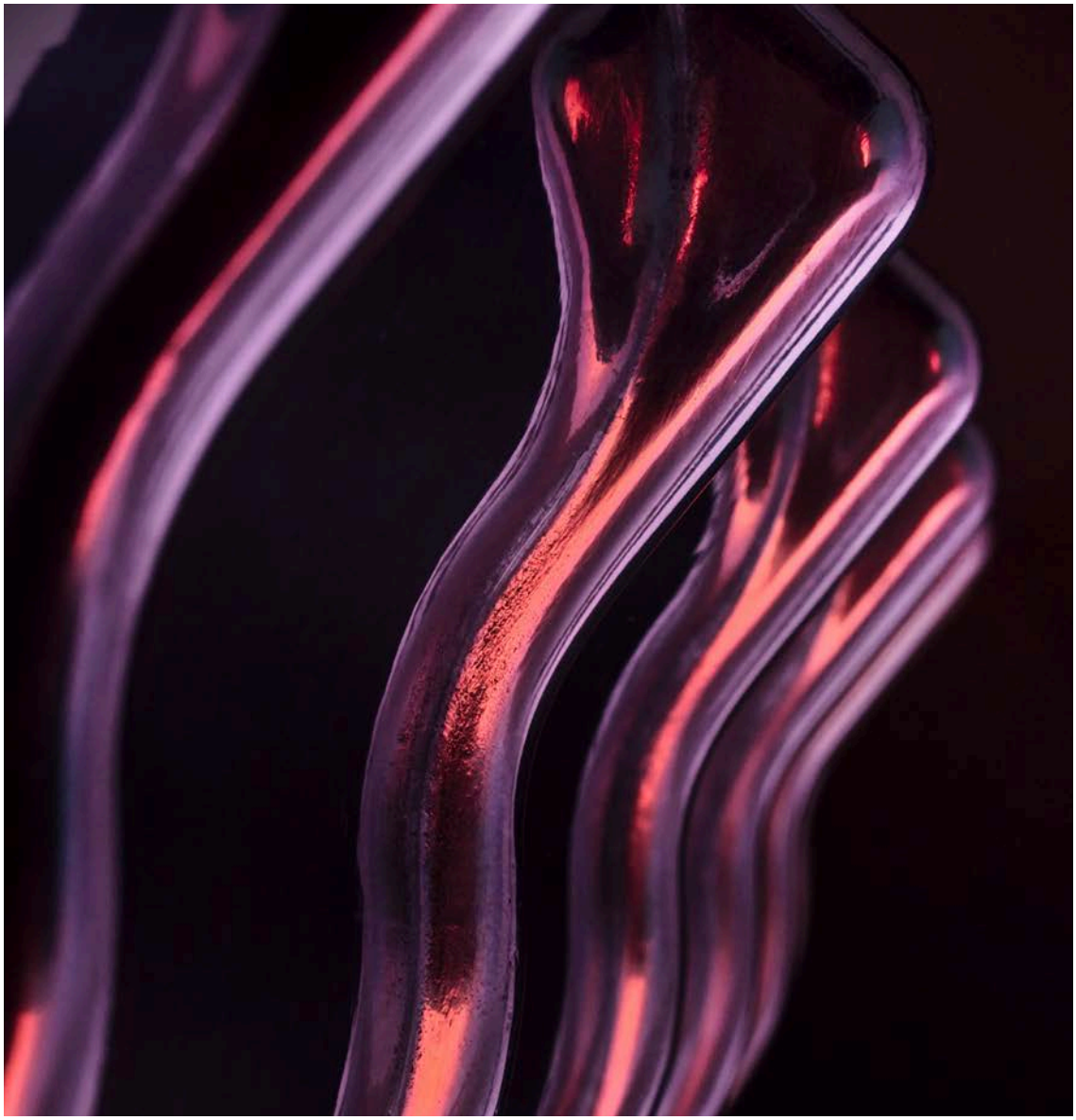
根据上述规定，即便引入人工智能辅助审方，药师本人也必须对处方进行审核。进一步根据《处方管理办法》的规定，药师在完成处方调剂后，应当在处方上签名或者加盖专用签章。因此，如果调剂后的处方无药师签章，或者虽有药师签章，但实际上药师并未审核，而是完全由人工智能进行的审核，则存在被认定为无药师审方的风险，可能被认定为未按照规定调剂处方药品，违反《处方管理办法》。

结语

整体上，人工智能在互联网诊疗领域的应用极大助力互联网诊疗的发展，对诊疗效率的提升毋庸置疑，不过，效率提升的同时，诊疗安全和诊疗质量的保障是应用人工智能技术的合规关键。尤其对于诊疗行为干预型智能技术，生产经营企业和互联网医院首先需谨慎进行属性界定，对于属于医疗器械的产品，应按照医疗器械的监督管理规则予以注册或备案；其次，在应用该类技术时，应同时注意遵循诊疗服务规范，不宜过度适用人工智能，人工智能在目前的定位宜偏向辅助功能，医师、药师、患者依然需审慎对待人工智能处理的结果。

傅长煜
合伙人
争议解决部
北京办公室
+86 10 5957 2085
fuchangyu@zhonglun.com

左玉茹
非权益合伙人
争议解决部
北京办公室
+86 10 5087 2996
zuoyuru@zhonglun.com



人工智能企业科创板上市重点法律问题

作者/熊川、王振、周玘荟

2021是“十四五规划”的开局之年，中国信通院在对“十四五纲要”的解读中提到：以人工智能为代表的新一代信息技术，将成为我国"十四五"期间推动经济高质量发展、建设创新型国家，实现新型工业化、信息化、城镇化和农业现代化的重要技术保障和核心驱动力之一。据蓝鲸财经报道，受到2020年新冠疫情的影响，人工智能企业迎来大爆发，企业争相布局AI+，多家人工智能企业接连启动IPO进程。与此同时，旨在聚焦支持“硬科技”的核心目标，科创板2021年以来也收紧了相关审查。本文总结了人工智能企业科创板上市的常见重点法律问题，供相关企业参考。

PART 01

委托开发、合作开发以及许可使用

人工智能行业属于技术密集型行业，人工智能企业技术往往以研发和技术为核心驱动力，较多人工智能企业存在与高校、科研机构、其他研发公司等进行合作研发或者委托研发的情况。

《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》第五十四条第三款规定：“发行人应披露正在从事的研发项目、所处阶段及进展情况、相应人员、经费投入、拟达到的目标；结合行业技术发展趋势，披露相关科研项目与行业技术水平的比较；披露报告期内研发投入的构成、占营业收入的比例。与其他单位合作研发的，还应披露合作协议的主要内容，权利义务划分约定及采取的保密措施等。”

对于存在委托研发、合作研发或是被许可、授权技术使用的企业，证券监管机构往往要求发行人披露协议主要内容，并关注相关技术成果/被许可技术是否涉及发行人核心技术，在发行人产品中的运用情况，相关成果的产权归属，发行人是否对相对方存在技术、人员上的依赖，双方是否存在纠纷或者潜在纠纷。此外，考虑到发行人多项产品和技术可能还处于研发阶段，相关核心技术无法通过专利形式予以保护，公司若不能采取有效措施保护核心技术，将面临技术泄密风险，因此证券监管部门往往还会关注发行人的保密措施是否到位。部分案例问询情况如下：

公司名称	披露文件	反馈内容
寒武纪/688256	关于中科寒武纪科技股份有限公司 首次公开发行股票并在科创板上市的补充法律意见书一/2020.05.07	三、关于发行人核心技术之“6.1 与中科院的技术授权、委托开发协议及人员兼职” 请发行人说明： (1)中科院计算所许可使用的知识产权在发行人产品中的具体应用情况，是否涉及核心技术、产品； (2)委托研发的分工及各自发挥的作用，中科院计算所授权发行人使用研发成果的期限、是否为独占许可，在发行人核心技术、产品中的运用情况；…… (5)结合前述技术授权、委托开发协议及人员兼职情况，分析发行人是否对中科院计算所存在人员、技术上的依赖，并充分揭示相关风险。
		四、关于发行人核心技术之“6.2 与边点科技的委托开发协议” 根据申报材料，2018年12月发行人委托EDGEFLARE TECHNOLOGY PTE.LTD.(边点科技)研发IP核，合同约定研发成果归发行人所有。2019年12月、2020年1月双方签署了补充协议，目前合同正在履行。 请发行人说明： (1)上述研发进展及成果运用情况，是否运用于发行人的核心技术、产品中，发行人是否存在对边点科技的技术依赖，相关技术的委托研发是否属于行业惯例； (2)边点科技对研发成果的使用情况，是否对发行人的业务开展造成不利影响，是否存在核心技术泄密的风险。
		五、关于发行人核心技术之“7.关于研发项目” 请发行人：(1)补充披露重大科研项目的研发形式、研发成果及归属、研发期间、主要参与人员，若为合作研发，请说明参与研发主体、各自发挥的作用、研发成果归属及使用约定、在发行人技术、产品中的运用情况等内容；(2)按照《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54条的规定补充披露技术储备情况。 请发行人律师对上述事项进行核查并发表明确意见。
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之一/2021.03.05	十一、关于核心技术及知识产权(《问询函》问题 16) 请发行人补充披露： (1)发行人参与重大专项科研项目的研发内容、项目进展、研发成果及归属情况，在发行人主要产品、核心技术中的运用情况； (2)合作研发项目的研发成果及归属情况、在发行人主要产品、

公司名称	披露文件	反馈内容
		核心技术中的运用情况，发行人在其中发挥的作用、是否存在对合作单位的技术依赖，采取的保密措施。 请发行人说明： （1）核心技术的形成过程、技术来源，是否存在技术、知识产权等方面的纠纷或潜在纠纷； （2）德领科技对重庆云从无形资产出资的具体内容及技术来源、发行人是否存在来源于中科院重庆绿色智能技术研究院或其它第三方主体的技术成果，前述无形资产及技术成果（如有）在发行人主要产品、核心技术中的运用情况及重要程度，发行人是否对前述单位构成技术依赖，发行人是否具备独立、可持续的研发能力；…… （5）继受取得专利的具体情况，包括受让原因及时间、转让方、转让价格及公允性、实际支付情况、是否存在纠纷或潜在纠纷，受让专利在发行人主要产品、核心技术中的运用情况； （6）上述专利质押的具体情况，包括质押专利名称、在发行人主要产品、核心技术中的运用情况及重要程度、相关借款及质押的履行情况，是否存在质押实现的风险及对发行人的影响，发行人是否存在其它未披露的资产抵质押情形； （7）发行人是否存在专利、软件著作权等的授权、许可情形，若存在，请说明具体情况。
依图科技/中止	关于Yitu Limited（依图科技有限公司）首次公开发行存托凭证并在科创板上市的补充法律意见书（一）/2021.02.10	十一、《问询函》第 20 题：熠知电子与芯片研发 请发行人披露：……（3）发行人报告期内的研发是否主要依赖熠知电子，收购熠知电子后，熠知电子是否存在人员流失情形，能否保证研发的持续性，发行人是否具有独立研发的能力；（4）发行人与熠知电子的历史合作关系，在第一代人工智能求索芯片的研发过程中各自发挥的作用，《知识产权共有协议》的主要内容，第一代人工智能求索芯片的具体应用情况，报告期内产生收入的具体情况；（5）第二代求索芯片的研发进展情况，依图网络与熠知电子提前终止《联合开发协议》的背景、原因，终止时的研发成果及归属安排，发行人与熠知电子及其少数股东之间是否存在纠纷或潜在纠纷。

PART 02

核心技术人员

人工智能企业作为典型的高科技创新企业，核心技术人员对其技术研发和企业发展有着较为关键的作用，科创板亦较为重视对核心技术人员的相关认定及披露。如《上海证券交易所科创板股票发行上市审核问答》（以下简称“**《审核问答》**”）第6问规定：“申请在科创板上市的企业，应当根据企业生产经营需要和相关人员对企业生产经营发挥的实际作用，确定核心技术人员范围，并在招股说明书中披露认定情况和认定依据。原则上，核心技术人员通常包括公司技术负责人、研发负责人、研发部门主要成员、主要知识产权和非专利技术的发明人或设计人、主要技术标准的起草者等。”《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》（以下简称“**《信息披露41号准则》**”）第五十四条第四款亦对核心技术人员的披露要求作出细致规定。

经检索相关人工智能企业案例，核心技术人员的稳定性，核心技术人员的认定标准，其在发行人专利研发中的作用，是否涉及违反与前任职单位的竞业禁止协议或者保密协议，其在发行人处的技术研发是否涉及前任职单位的技术成果，是否存在纠纷或者潜在纠纷等往往是证券监管部门的关注要点。部分案例问询情况如下：

公司名称	披露文件	反馈内容
虹软科技/688088	关于虹软科技股份有限公司首次公开发行人民币普通股(A 股)股票并在科创板上市之补充法律意见书（二）/2019.05.23	问题11：关于知识产权 请发行人：……（2）说明实际控制人、董事、高级管理人员、核心技术人员是否存在违反与曾任职单位之间的竞业禁止协议或保密协议的情况……（5）D某与Z某发明专利数占公司所有发明专利比例高于10%，两人已于2005年从公司离职，以上两人离职的原因，是否与发行人在专利权属方面存在纠纷……
旷视科技/已问询	关于MEGVII TECHNOLOGY LIMITED（旷视科技有限公司）首次公开发行中国存托凭证并在科创板上市的补充法律意见书（一）/2021.05.28	问题 9 关于公司董监高及核心技术人员 根据招股说明书，公司高管付某、孙某在发行人处任职之前曾任职其他研究单位，同时发行人核心技术人员包括范某、周某等人。 请发行人说明：（1）付某、孙某等人到发行人处履职是否存在违反前任职单位保密协议、竞业禁止的规定的情形；是否存在带有相关职务发明或技术入职发行人的情形；是否存在纠纷或潜在纠纷；（2）结合发行人的技术研发和专利、奖项获得情况，说明核心技术人员认定的标准；当前核心技术人员和发行人的专利、所获奖项之间的对应关系。
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之一/2021.03.05	请发行人说明：（1）董监高、核心技术人员及其他相关人员是否存在违反原任职单位关于竞业禁止、保密协议约定的情形，发行人核心技术、产品的研发是否涉及其原任职单位的技术成果，与原单位是否存在纠纷或潜在纠纷；
云天励飞/已问询	关于深圳云天励飞技术股份有限公司首次公开发行股票并在科创板上市的补充法律意见书（一）/2021.03.12	问题七（问询函“一、关于发行人股权结构、董监高等基本情况/5.关于核心技术人员”）： 请发行人说明： （1）王某自2017年加入公司以来的薪酬变动情况，薪酬确定方式，是否存在相应的考核制度，薪酬明显高于其他董监高和核心技术人员的原因和合理性，是否履行相应的决策程序，是否存在潜在利益安排；王某在发行人生产经营中所发挥的作用及担任职务情况，其加入公司前后在相关技术、生产经营等方面是否存在变化； （2）王某是否与发行人控股股东、实际控制人、董监高及其亲属、主要客户、供应商存在关联关系、业务往来以及其他利益安排； （3）发行人核心技术人员是否存在违反原任职单位关于竞业禁

公司名称	披露文件	反馈内容
		止、保密协议约定的情形，发行人核心技术、产品的研发是否涉及其原任职单位的技术成果，是否存在纠纷或潜在纠纷。
依图科技/中止	关于Yitu Limited（依图科技有限公司）首次公开发行存托凭证并在科创板上市的补充法律意见书（一）/2021.02.10	七、《问询函》第 8 题：关于董事及核心技术人员 招股说明书披露，最近两年公司董事变化较大，朱某、林某和吕某三人为公司核心技术人员。 请发行人披露：（2）核心技术人员的认定依据，是否包括公司技术负责人、研发负责人、研发部门主要成员、主要知识产权和非专利技术的发明人或设计人、主要技术标准的起草者等；（3）最近两年内董事、核心技术人员是否发生重大不利变化；（4） 发行人的高级管理人员、核心技术人员是否存在违反原任职单位关于竞业禁止、保密协议约定的情形，发行人核心技术、产品的研发是否涉及其原任职单位的技术成果，是否存在纠纷或潜在纠纷。

此外，企业部分核心技术人员可能来自于中科院等事业单位，因此除上述关注点外，还可能涉及相关任职资格限制、研发成果归属问题。

如寒武纪申报材料披露，报告期内有27名中科院计算所智能处理器中心员工在发行人处兼职，主要担任工程师，从事研发相关工作，其实际控制人陈某及核心技术人员刘某于2018年4月在中科院计算所办理了离岗创业手续，2019年从中科院计算所离职。针对该问题，证券监管部分连续两次追问相关情况，第一次要求说明："（3）上述27人在发行人处及中科院计算所的任职情况，是否存在处级以上事业单位人员，是否符合事业单位人员兼职的相关规定；（4）中科院计算所对离岗创业人员、兼职人员在创业、兼职期间形成科技成果或知识产权的相关规定，上述人员目前取得研发成果的情况，相关成果归属于中科院计算所还是发行人；"，第二次针对兼职人员中有职级的工程师进一步发问，要求"核查郭某是否属于《中国科学院工作人员兼职管理规定》所规定的在任的所（局）级领导干部以及具有事业法人资格的院属处级单位领导干部，仅取得中科院计算所出具的书面确认、未取得上级批准文件是否符合要求。"云从科技申报材料亦披露其部分董事、高管，以及3名核心技术人员中的2名均曾在中科院重庆绿色智能技术研究院任职，因此证券监管部门要求其披露并说明"（3）除上述人员外，发行人是否存在其他员工来自于中科院重庆绿色智能技术研究院或进行兼职的情形，如有，目前

在发行人的任职情况，兼职人员是否符合相关兼职管理规定；……（3）董监高中是否存在处级以上事业单位人员，是否符合事业单位人员兼职的相关规定；……”

PART 03

贸易保护政策影响

根据美国《出口管理条例》，美国商务部可通过将某些实体或个人列入“实体清单”的方式，限制对其的出口，任何人向实体清单上的实体或者个人出口被管制货物前，均需预先从美国商务部获得出口许可，而商务部实行假定拒绝原则，原则上拒绝批准许可。

我国较多人工智能企业如科大讯飞、商汤科技、旷世科技、依图科技、云从科技、颐信科技等均被列入了美国实体清单，因此，若是相关人工智能企业涉及境外进口相关原材料，可能会被证券监管机构关注贸易保护政策风险，如要求披露涉及境外进口的原材料的类型、金额、是否涉及发行人产品核心零部件等具体信息，要求说明相关贸易保护政策对发行人产品核心原材料稳定性的影响，是否会对发行人持续经营构成重大不利影响，以及发行人是否有相应替代措施、未来境外业务计划等。部分案例问询情况如下：

公司名称	披露文件	反馈内容
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之一/2021.03.05	八、关于贸易保护政策（《问询函》问题 11） 招股说明书披露，（1）云从科技于2020年5月被美国商务部列入“实体清单”；（2）2018年11月26日，发行人设立了全资子公司云从（美国）信息科技有限公司，旨在通过该境外子公司与人工智能领域专业实验室开展人工智能理论研究和学术交流。 请发行人披露： （1）被纳入“实体清单”对发行人生产经营的具体限制； （2）涉及境外厂商生产的原材料的具体类型、金额及其占比、直接供应商及最终供应商名称，是否构成产品的核心零部件； （3）如何保障生产所需的核心原材料的稳定性，如果因贸易摩擦等事项导致无法正常采购该等核心器件是否会对持续经营构成重大不利影响，是否有相应的替代措施； （4）报告期内发行人未拓展境外业务的原因、未来的境外业务拓展计划，云从美国报告期内业务经营、研究活动等的开展情况，纳入“实体清单”后对公司境外业务拓展及云从（美国）业务开展的影响及应对措施。

公司名称	披露文件	反馈内容
	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之二/2021.06.25	八、关于贸易保护政策（《问询函》问题 6） 根据首轮问询回复，报告期内公司向境内厂商采购的模组、服务器等部分采购的硬件中包含英特尔、安森美等美国公司的芯片、显卡等器件，属于《美国出口管制条例》管控范围内的美国境外制造的美国原产比例高于25%的产品。 请发行人说明：公司采购材料中包含的境外厂商生产器件是否属于发行人产品的核心零部件，量化分析并补充披露因纳入“实体清单”或贸易摩擦等事项导致无法正常采购该等核心器件对发行人生产经营的影响，是否构成重大不利影响，完善重大事项提示的相关内容。 请保荐机构、发行人律师对上述事项进行核查并发表明确意见。
依图科技/中止	关于Yitu Limited（依图科技有限公司）首次公开发行存托凭证并在科创板上市的补充法律意见书（一）/2021.02.10	十、《问询函》第19题：关于贸易保护政策 招股说明书披露，依图网络于2019年10月8日被美国商务部列入“实体清单”。请发行人披露： （1）涉及境外厂商生产的原材料的具体类型、金额及其占比、直接供应商及最终供应商名称，是否构成产品的核心零部件； （2）如何保障生产所需的核心原材料的稳定性，如果因贸易摩擦等事项导致无法正常采购该等核心器件是否会对持续经营构成重大不利影响，是否有相应的替代措施； （3）报告期内IP和EDA工具授权使用的情况，包括授权主体、授权时间、授权费用、到期后的续约安排等，如果无法持续使用对公司经营是否构成重大不利影响。 请保荐机构、发行人律师结合上述事项，就依图网络被美国商务部列入“实体清单”对持续经营的具体影响进行核查，并发表明确意见。请发行人就依图网络被美国商务部列入“实体清单”事项及对持续经营的影响进行重大事项提示。
旷视科技/已问询	关于MEGVII TECHNOLOGY LIMITED（旷视科技有限公司）首次公开发行中国存托凭证并在科创板上市的补充法律意见书（一）/2021.05.28	问题21 关于贸易政策的影响 根据招股说明书，2019年10月9日，美国商务部以“实体被合理地认为涉及有违美国外交政策利益的活动”为由，将包括本公司在内的28家中国实体列入《出口管制条例》（EAR）实体清单。发行人从美国或其他国家进口美国原产的商品、技术或软件受到限制。 请发行人披露： （1）被纳入“实体清单”对发行人生产经营的具体限制； （2）涉及境外厂商生产的原材料的具体类型、金额及其占比、相关供应商的名称等，该等原材料是否构成产品的核心零部件；

公司名称	披露文件	反馈内容
		(3)如何保障生产所需的核心原材料的稳定性，如果因贸易摩擦等事项导致无法正常采购该等核心器件是否会对持续经营构成重大不利影响，是否有相应的替代措施； (4)报告期内发行人境外销售的具体地区、产品等基本情况；未来的境外业务拓展计划；相关境外子公司报告期内业务经营、研究活动等的开展情况，纳入“实体清单”后对公司境外业务拓展的影响及应对措施。

PART 04

数据来源及合规性

随着《中华人民共和国数据安全法》(2021年6月10日经第十三届全国人民代表大会常务委员会第二十九次会议通过，于2021年9月1日起实施)《个人信息保护法(草案二次审议稿)征求意见稿》(2021年4月29日经第十三届全国人大常委会第二十八次会议通过)等出台，数字经济时代下对数据安全和个人信息的保护与监管日益趋严，而人工智能企业的技术及产品往往会涉及数据、个人信息的采集、运用等，因此证券监管部门对数据合规较为关注，其关注要点包括数据来源及其合法合规性，数据使用的合规性，是否建立了数据存储和保密的管理制度并能有效执行，是否涉及数据合规方面的诉讼及纠纷等。部分案例问询情况如下：

公司名称	披露文件	反馈内容
旷视科技/已问询	关于MEGVII TECHNOLOGY LIMITED(旷视科技有限公司)首次公开发行中国存托凭证并在科创板上市的补充法律意见书(一)/2021.05.28	问题 20 关于数据合规及科技伦理 根据招股说明书，发行人的AI核心技术中包括系统层及算法层，涉及数据的处理、清洗和管理能力，算力的共享、调度和分布式能力，以及算法的训练、推理及部署能力。 请发行人说明：(1)发行人技术、业务及产品(或服务)中涉及到数据采集、清洗、管理、运用的具体环节；不同环节涉及的数据的具体类型，文字、图像、视频等具体情况；(2)发行人自身核心技术(如算法的训练、系统的搭建等)是否涉及大量的数据的应用，如是，相关数据的来源及其合规性；(3)发行人对外提供的产品(或服务)是否涉及数据的采集运用，如是，说明数据的来源及其合法合规性；(4)发行人保证数据采集、清洗、管理、运用等各方

公司名称	披露文件	反馈内容
		面的合规措施；(5) 发行人的数据来源中是否包含向供应商采购，如是，请说明是否在相关合同中约定数据合规的条款或措施，并结合《民法典》《网络安全法》和《个人信息安全规范》《数据安全法（草案）》（已于2021年6月10日正式通过）《个人信息保护法（草案）》等相关规定，说明相关措施是否能切实保证发行人不出现数据合规风险或法律纠纷；(6) 结合发行人的产品交付及部署模式，说明发行人的产品（或服务）中涉及到用户的个人数据的情形和场景，该等数据的运用、管理及其合规性；(7) 发行人产品至今是否面临数据合规方面的诉讼或纠纷；并请结合相关公开报道，说明发行人数据的合规性。
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之二/2021.06.25	七、关于数据来源及其合规性（《问询函》问题 3） 根据首轮问询回复，人工智能行业当前技术主要以深度学习技术为核心，通过大量数据的训练学习，实现机器对于任务的自主化学习。近期部分地方立法对个人信息采集和人脸识别应用范围进行约束，对企业在数据应用合规性、数据安全技术上提出更高要求，人工智能的应用难度会逐步提升。 请发行人说明：(1) 近期立法对个人信息采集和人脸识别应用范围等进行约束的具体体现，对发行人业务开展的影响，是否存在违反相关规定的情形；(2) 发行人产品的研发、生产及使用过程中涉及到的数据获取、使用情况，数据获取方式及其合规性，是否获得相关数据主体的明确授权许可，授权许可是否存在使用范围、主体或期限等方面的限制，发行人是否存在超出上述限制使用数据的情形，是否存在获取、使用相关数据时侵犯个人隐私或其他合法权益的情形，发行人业务开展及人脸信息收集等是否符合《个人信息安全规范》等相关法律法规的规定，是否存在纠纷或潜在纠纷，相关风险揭示是否充分。 请保荐机构、发行人律师对上述事项进行核查并发表明确意见。
云天励飞/已问询	关于深圳云天励飞技术股份有限公司首次公开发行股票并在科创板上市的补充法律意见书（一）/2021.03.12	问题十一（问询函“二、关于发行人业务/11.关于行业政策和数据使用/11.2”）： 根据申报材料：公司当前主营业务收入主要来源于公司在数字城市运营管理及人居生活智慧化升级各应用场景中，为下游客户提供的“端云结合”的整体AI 赋能方案。 请发行人说明：(1) 清晰说明发行人业务开展过程中涉及到相关个人数据、信息安全的获取、利用及保护的情况；(2) 视觉人工智能技术的初始训练、迭代更新、模型训练上所需的大量数据的具

公司名称	披露文件	反馈内容
		体来源，发行人在场景应用过程中是否接触、收集、利用人脸数据信息，数据采集和使用过程中是否获得被收集者许可，是否存在侵犯个人隐私、肖像权等权益的情形，发行人业务开展过程中涉及到数据获取、管理和使用是否合法合规，发行人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，发行人是否需要取得开展涉密类业务的资质或许可。 请发行人律师对上述事项进行核查并发表明确意见。

PART 05

股东和特殊权利

人工智能作为近年来的新兴产业，相关企业设立较晚，运营时间较短，但同时又具有业务发展迅速、融资频繁的特点，对于报告期内存在多次股本变动、股东变动的，证券监管部门可能会予以关注。关注要点包括增资或股权转让的原因及合理性，是否履行了必要的程序，增资或股权转让价格的公允性、合理性，价款支付情况以及税费缴纳情况，相关资金来源及合法性，新增股东的基本情况以及与发行人董监高、员工、客户和供应商等是否存在关联关系或其他可能导致利益输送的关系，是否存在委托持股、信托持股、对赌或其他特殊利益安排，以及该等安排对发行人股权稳定性、持续经营等的影响。

此外，对于部分新增股东为国有企业或其他投融资受有相关限制的特殊行业企业，还应当关注其投资于发行人是否符合相关规定，是否履行了相应的程序等，如云从科技首轮问询中，监管机构要求其说明“国有股东入股发行人及股权变动是否履行评估、备案等程序，是否符合相关法律法规的规定，是否造成国有资产流失；”旷视科技首轮问询中，监管机构要求其说明：“当前对于银行、保险等国有金融行业关于对外投融资的相关规定，并进一步说明“阳光人寿保险股份有限公司”“China Harvest Limited”“ICBC AMG China Fund I SPC”及其他类似特殊行业投资发行人是否符合相关规定，投资决策、资金来源、投资比例等，是否合法合规，是否存在违规事项。”

公司名称	披露文件	反馈内容
虹软科技/688088	关于虹软科技股份有限公司首次公开发行人民币普通股(A 股)股票并在科创板上市之补充法律意见书（三）/2019.05.31	问题2：关于对赌安排 请发行人进一步说明： （1）2017年9月增资签署的《补充协议》、《虹软（杭州）多媒体信息技术有限公司之补充协议（二）》包含的业绩目标及估值调整条款的具体内容及法律效力、两份协议是否终止，如未终止，是否符合《上海证券交易所科创板股票发行上市审核问答（二）》（上证发〔2019〕36号）（以下简称《问答（二）》）的要求、是否存在其他替代性利益安排； （2）2018年5月及9月已终止的对赌安排是否彻底终止、是否为附条件终止、是否存在其他替代性利益安排； （3）发行人是否存在其他特殊权利安排，如有，相关安排是否符合《问答（二）》的要求； （4）结合上述协议的法律状态及其他或有特殊利益安排，说明实际控制人邓晖持有的发行人股份权属是否清晰、稳定。请发行人提供上述对赌协议、终止协议、相关对赌方的书面确认等文本。请保荐机构、发行人律师核查上述事项，并发表明确意见。
旷视科技/已问询	关于MEGVII TECHNOLOGY LIMITED（旷视科技有限公司）首次公开发行中国存托凭证并在科创板上市的补充法律意见书（一）/2021.05.28	问题 6 关于股东核查及历史沿革 根据招股说明书及股东核查情况，发行人历次外部融资过程中，API（Hong Kong）Investment Limited（以下简称：API）较其他股东存在较大差异。 请发行人说明： （1）上述低价转让的背景原因及其合理性，其他投资人是否知晓并同意，是否违反融资协议相关条款，是否存在纠纷或潜在纠纷，结合与阿里巴巴业务合作情况，分析相关股权转让行为是否构成股份支付，相关会计处理是否符合《企业会计准则》； （2）结合 API 背后的投资主体与发行人的具体业务合作关系，说明低价向其转让股权是否存在利益输送；双方是否存在其他利益安排； （3）请根据证监会《监管规则适用指引——关于申请首发上市企业股东信息披露》的规定，进一步完善股东核查事项； （4）上述间接股东中工会持股的情况请参考《审核问答（二）》问题 1 的要求进行相关核查和披露； （5）梳理发行人股东中符合返程投资要求的股东情形并说明是否均办理相关登记及合法合规情况。

公司名称	披露文件	反馈内容
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之一/2021.03.05	三、关于股东（《问询函》问题 2） 请发行人说明： （1）列表说明历次股权变动的原因、交易价格及公允性、款项支付情况及缴纳时点、税收缴纳情况，增资或入股资金来源及合法性；同一时间段价格差异较大的原因及合理性；2016年1月增资价格与2015年12月和2016年6月增资价格差异较大的原因及合理性、增资股东的基本情况，是否存在利益输送情形； （2）报告期内入股股东的基本情况，入股原因，与发行人业务开展之间的关系，入股前后发行人业务的变化情况，与发行人董监高、员工、客户和供应商等是否存在关联关系或其他可能导致利益输送的关系，发行人股东是否存在委托持股、信托持股或其他特殊利益安排； （3）部分实缴出资时间早于股东会决议的原因及合理性，更换多个员工持股平台持股发行人的原因及合理性，退出的员工持股平台存续状态及未来计划安排； （4）14家机构股东是否存在应当办理而未办理备案的情形； （5）自然人股东的履历情况，入股发行人的原因，是否与发行人及其关联方、客户、供应商等存在关联关系、业务、资金往来或其他特殊利益安排； （6）国有股东入股发行人及股权变动是否履行评估、备案等程序，是否符合相关法律法规的规定，是否造成国有资产流失……
	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之二/2021.06.25	请发行人披露：除抚州友邦、广东创投、南沙金控、深圳兴旺等股东外，其他股东与发行人及其控股股东、实际控制人签署的特殊权利条款解除后是否约定有恢复条款，并完善关于对赌安排的风险提示内容。
依图科技/中止	关于Yitu Limited（依图科技有限公司）首次公开发行存托凭证并在科创板上市的补充法律意见书（一）/2021.02.10	六、《问询函》第 7 题：关于最近一年新增股东 请发行人披露最近一年新增股东的增资或者受让股份的价格、定价依据及其公允性，价格存在差异的，原因及合理性，是否存在利益输送情形。

公司名称	披露文件	反馈内容
云天励飞/已问询	关于深圳云天励飞技术股份有限公司首次公开发行股票并在科创板上市的补充法律意见书(一)/2021.03.12	问题四(问询函“一、关于发行人股权结构、董监高等基本情况/2.关于历史沿革”): 请发行人说明:(1)发行人设立及增资涉及相关货币和知识产权出资是否到位,是否履行必要的程序,出资知识产权在发行人生产经营中的作用及重要性,是否存在出资不实等情形,是否符合法律法规规定,2020年陈某置换历史上知识产权出资的原因;……(3)报告期内频繁融资的必要性,资金用途及去向,入股股东与报告期内发行人主要客户、供应商是否存在关联关系、业务往来或其他利益安排;(4)报告期内历次增资或股权转让定价依据及合理性,相近或相同批次增资或股权转让价格差异较大的原因及合理性,资金来源、相关价款支付情况及税费缴纳情况,是否涉及未披露的其他利益安排及具体情况,发行人股权是否存在纠纷或潜在纠纷风险;(5)历史上国资股东入股及退出是否履行了完整必备的法定程序,是否符合国资相关法律法规规定,是否存在国有资产流失的情形;(6)发行人历次股权转让和整体变更过程中涉及的股东个人所得税缴纳情况,是否存在税务合规风险。

PART 06

业务资质、许可

应用层人工智能企业的相关产品往往应用于各个领域,如AI+交通,AI+金融,AI+医疗等,就特定领域和业务而言,企业可能需要取得相应资质,如增值电信业务相关许可证、智能化建筑业务领域的相关许可等。IPO实践中,证券监管部门亦会例常关注企业的业务资质情况,要求企业说明其是否已经取得了业务开展所必需的资质,对于部分涉及外资成分的企业,证券监管部门还会关注企业的业务是否属于外商投资准入负面清单禁止业务。部分案例问询情况如下:

公司名称	披露文件	反馈内容
旷视科技/已问询	关于MEGVII TECHNOLOGY LIMITED（旷视科技有限公司）首次公开发行中国存托凭证并在科创板上市的补充法律意见书（一）/2021.05.28	35.6 根据招股说明书……发行人开展业务需要取得相关资质。请发行人说明：…… （2）发行人报告期内开展业务是否均取得相应的资质，是否存在相应的违法违规情形。
云天励飞/已问询	关于深圳云天励飞技术股份有限公司首次公开发行股票并在科创板上市的补充法律意见书（一）/2021.03.12	请发行人说明：……（2）发行人从事安防等相关场景业务是否需要具备相关资质 ；结合公司所有即将到期的资质情况，进一步说明相关资质到期后对公司业务经营的影响，公司采取的相关应对措施。
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之一/2021.03.05	十、关于资源要素（《问询函》问题 15） 请发行人说明：……（2）发行人及其子公司主营业务与所需经营资质的对应关系，云从有限高新技术企业证书的续期进展，是否存在无法续期的障碍及对发行人的影响；（3）发行人是否已经取得所从事业务的全部资质，是否存在未取得相关业务资质前开展生产经营的情形；（4）发行人业务是否属于外商投资准入负面清单禁止业务，如属于，发行人是否存在外资股东，如存在，相关经营是否合法法规。
依图科技/中止	关于Yitu Limited（依图科技有限公司）首次公开发行存托凭证并在科创板上市的补充法律意见书（一）/2021.02.10	十二、《问询函》第 21 题：关于业务资质 根据招股说明书披露，发行人部分业务资质在 2019 年才取得，取得时间较晚。 请保荐机构、发行人律师：（1）就发行人是否已经取得所从事业务的全部资质，是否存在未取得相关业务资质前开展生产经营的情形进行核查，并发表明确意见；（2）核查发行人业务是否属于外商投资准入负面清单禁止业务，如属于，请作相应的重大事项提示。

PART 07

租赁

经检索相关IPO案例，存在较多人工智能企业无自有房产的情况，此时证券监管部门可能会关注租赁相关情况，如租赁房产是否办理租赁备案，房产实际用途与法定用途是否一致，租赁房产是否取得相应产权证书，是否存在未经出租人同意转租的情形，是否存在纠纷或潜在纠纷以及前述瑕疵是否可能导致发行人受到行政处罚、该等处罚对发行人持续经营的影响等。部分案例问询情况如下：

公司名称	披露文件	反馈内容
旷视科技/已问询	关于MEGVII TECHNOLOGY LIMITED（旷视科技有限公司）首次公开发行中国存托凭证并在科创板上市的补充法律意见书（一）/2021.05.28	**35.6 根据招股说明书，发行人存在租用房产未租赁备案以及未取得权利人同意使用擅自转租的房产的情形。请发行人说明：** **（1）上述房产租赁瑕疵是否得到消除，未消除的是否构成违法违规事项，以及对发行人生产经营的影响；**
虹软科技/688088	关于虹软科技股份有限公司首次公开发行人民币普通股（A 股）股票并在科创板上市之补充法律意见书/2019.04.30	**问题22：** **截至招股说明书签署日，发行人共租赁房产22处。请发行人补充披露：** **（1）上述租赁房屋的实际用途，与法定用途是否相符，是否存在因违法违规被行政处罚的风险。** **（2）租赁尚未取得权属证书的房产或租赁未经所有权人同意转租的房产进行办公、生产经营是否存在纠纷或潜在纠纷，是否存在行政处罚风险，如果搬迁对公司持续经营的影响，相关补救措施。** **（3）补充披露相关租赁是否办理租赁备案登记手续，如未办理对相关租赁合同效力的影响，是否存在行政处罚风险。** **请保荐机构和发行人律师对上述事项进行核查，同时请结合相关租赁房屋的具体用途、对发行人的重要程度、租赁费用的公允性、租赁期限、到期后的续约安排、发行人的处置方案等，对上述事项是否对发行人的资产完整性构成重大不利影响发表明确意见。**

公司名称	披露文件	反馈内容
云从科技/已问询	关于云从科技集团股份有限公司申请首次公开发行股票并在科创板上市的补充法律意见书之一/2021.03.05	十、关于资源要素(《问询函》问题 15) 根据申报材料,发行人无自有房产,生产经营场所通过租赁取得;主要经营资质中各子公司的资质存在差异,云从有限的高新技术企业证书已于 2020 年 12月 10 日到期。 请发行人说明:(1)租赁房屋是否存在与法定用途不一致的情形、是否租赁集体土地用地或划拨用地,是否取得相应产权证书,是否存在未经出租人同意转租的情形,是否存在纠纷或潜在纠纷;

PART 08

关于科创属性的要求

(一)科创属性基本要求

1.行业要求

(1)鼓励新一代技术领域人工智能技术

根据《上海证券交易所科创板企业发行上市申报及推荐暂行规定》,企业在科创板发行上市的,需要符合科创属性的要求,把握发行人是否符合科创板的定位。具体来说,科创属性包括行业要求和指标要求,行业要求中[1],人工智能属于新一代信息技术领域,是科创板定位中支持及鼓励的行业。

(2)需要结合人工智能应用行业领域、技术先进性水平综合判断

值得注意的,是人工智能主要是一种技术手段,往往与具体业务共生。因此,除了公司采用人工智能技术外,同时,还需要考虑对应具体行业情况。例如,如果人工智能应用于限制上市的行业领域,比如涉及属于"限制金融科技、模式创新企业在科创板发行上市。禁止房地产和主要从事金融、投资类业务的企业",那么,我们理解在该等企业科创板上市方面会受到一定的限制。

除此外,尽管行业符合相关要求,但同时也需要进一步关注公司技术能力是否领先的问题,尤其是在要求"硬科技"的政策背景下,公司在申请上市及上市反馈回复中,监管往往会重点关注公司技术先进性的问题。如果公司人工智能技术先进性水平不够领先或市场可替代性很强,那么也可能会被审核人员认为不符合科创属性,要求或建议公司撤回上市申请。

2.基本指标要求

根据《上海证券交易所科创板企业发行上市申报及推荐暂行规定(2021

1.《上海证券交易所科创板企业发行上市申报及推荐暂行规定(2021年4月修订)》第四条规定:"申报科创板发行上市的发行人,应当属于下列行业领域的高新技术产业和战略性新兴产业:(一)新一代信息技术领域,主要包括半导体和集成电路、电子信息、下一代信息网络、人工智能、大数据、云计算、软件、互联网、物联网和智能硬件等;(二)高端装备领域,主要包括智能制造、航空航天、先进轨道交通、海洋工程装备及相关服务等;(三)新材料领域,主要包括先进钢铁材料、先进有色金属材料、先进石化化工新材料、先进无机非金属材料、高性能复合材料、前沿新材料及相关服务等;(四)新能源领域,主要包括先进核电、大型风电、高效光电光热、高效储能及相关服务等;(五)节能环保领域,主要包括高效节能产品及设备、先进环保技术装备、先进环保产品、资源循环利用、新能源汽车整车、新能源汽车关键零部件、动力电池及相关服务等;(六)生物医药领域,主要包括生物制品、高端化学药、高端医疗设备与器械及相关服务等;(七)符合科创板定位的其他领域。限制金融科技、模式创新企业在科创板发行上市。禁止房地产和主要从事金融、投资类业务的企业在科创板发行上市。"

年4月修订）》《科创属性评价指引（试行）》等规定，除了行业符合相关要求外，同时也应该符合科创属性的相关指标要求，具体指标要求如下：

“同时符合下列4项指标：

1. 最近三年研发投入占营业收入比例5%以上，或最近三年研发投入金额累计在6000万元以上；

2. 研发人员占当年员工总数的比例不低于10%；

3. 形成主营业务收入的发明专利5项以上；

4. 最近三年营业收入复合增长率达到20%，或最近一年营业收入金额达到3亿元。”

其中，采用《上海证券交易所科创板股票发行上市审核规则》第二十二条第（五）款规定的上市标准[2]申报科创板的企业可不适用上述第4项指标中关于“营业收入”的规定，“（一）虽未达到签署指标，但符合下列情形之一：

1. 发行人拥有的核心技术经国家主管部门认定具有国际领先、引领作用或者对于国家战略具有重大意义；

2. 发行人作为主要参与单位或者发行人的核心技术人员作为主要参与人员，获得国家科技进步奖、国家自然科学奖、国家技术发明奖，并将相关技术运用于公司主营业务；

3. 发行人独立或者牵头承担与主营业务和核心技术相关的国家重大科技专项项目；

4. 发行人依靠核心技术形成的主要产品（服务），属于国家鼓励、支持和推动的关键设备、关键产品、关键零部件、关键材料等，并实现了进口替代；

5. 形成核心技术和主营业务收入的发明专利（含国防专利）合计50项以上。”

对于上述业务指标，需要特别注意的是，人工智能往往是以技术方式呈现，而很多企业并未申请到与主营业务密切相关的5项专利技术。在此背景下，若公司结合自身情况将自身定位于软件行业，而我们理解科创属性中关于“软件企业”主要是为研发生产基础性软件的企业（比如office办公系统）。如果公司不属于典型的软件企业，这很可能会受到监管的挑战，并进一步认定公司不符合科创属性。

（二）部分审核案例问询情况

经检索相关IPO案例，证券监管部门亦会质疑科创板申报企业在《招股说明书》中披露的内容不足以充分说明自身符合科创属性的要求而在上市审核的反馈中就相关情况进行问询，部分人工智能企业被问询的案例情况

2.预计市值不低于人民币40亿元，主要业务或产品需经国家有关部门批准，市场空间大，目前已取得阶段性成果。医药行业企业需至少有一项核心产品获准开展二期临床试验，其他符合科创板定位的企业需具备明显的技术优势并满足相应条件。

如下：

公司名称	披露文件	反馈内容
易来智能/已问询	发行人及保荐机构第二轮审核问询函回复报告	**在“关于科创属性”的问题下，证券监管部门又细分为四个小问题进行问询，分别为“关于技术先进性”、“关于行业地位”、“关于市场竞争状况”、“关于科创板支持方向”等，让发行人及中介机构多角度地论证公司是否符合科创属性。**
赛赫智能/已问询	关于赛赫智能设备（上海）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第三轮审核问询函的回复	**问题1 关于科创属性问题** **问题1.1　发行人在二轮问询回复中将形成主营业务收入发明专利数量改为13项，其中境内发明专利5项，境外发明专利8项。公司有10项发明专利为受让取得。公司有3项发明专利为项目受理后取得。公司VFM变频微波固化产品基于LambdaTechnologies,Inc的专利授权进行研发，2019年11月研发完毕，2020年1月测试阶段结束，进入量产阶段，在报告期内尚未产生收入。后续LambdaTechnologies,Inc将相关发明专利转让给发行人。** **请发行人进一步说明（1）公司发明专利在具体产品中的应用情况，实现的销售收入情况；（2）公司发明专利与核心技术的对应关系，所起的作用，是否实际应用于核心技术和产品中；（3）VFM变频微波固化产品尚未产生收入的情况下，相关发明专利即形成主营业务收入的真实性、合理性；（4）公司多项发明专利为申报后取得相关发明专利的取得方式、取得过程；（5）发行人形成主营业务收入发明专利数量的披露是否真实、准确。** **问题 1.2** **关于行业，根据二轮问询回复，发行人主营业务属于国家统计局发布的《战略性新兴产业分类（2018）》规定的战略新兴产业，如轻量化车身成型技术的研发与应用属于“5.4.2新能源汽车其他相关服务”，或属于国家发展改革委发布的《产业结构调整指导目录（2019 年本）》规定的鼓励类产业。** **请发行人进一步说明：（1）公司轻量化车身成型技术的研发与应用属于《战略性新兴产业分类（2018）》“5.4.2新能源汽车其他相关服务”的依据，整车下线检测系统、总装电检系统属于《战略性新兴产业分类（2018）》“2.1.3智能测控装备制造”的依据；（2）公司产品属于《产业结构调整指导目录 2019年本）》的依据；（3）发行人属于重点推荐领域“高端装备领域”中“智能制造”细分领域的依据是否充分，若否，请修改行业定位。**

公司名称	披露文件	反馈内容
		问题 1.3 申报文件显示，报告期内，公司核心技术产品收入占主营业务收入的比例为 94.04%、92.58%、97.77%、98.57%。二轮回复后都改为 100%。 请发行人说明： （1）结合合同条款，长春吉文冲压生产线项目是否属于贸易类业务，是否属于核心技术收入； （2）前后信息披露不一致的原因，公司核心技术产品收入占主营业务收入比例的计算过程、依据，信息披露是否真实准确、完整。
康代智能/终止审核	发行人及保荐机构关于苏州康代智能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第一轮审核问询函的回复（2020年半年报财务数据更新版）	招股说明书披露：发行人符合《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第五条规定的“（四）依靠核心技术形成的主要产品（服务），属于国家鼓励、支持和推动的关键设备、关键产品、关键零部件、关键材料等，并实现了进口替代”。发行人自动光学检测解决方案的底层机器视觉算法、关键组件等均由公司自主研发设计，产品的关键指标达到了国际先进水平，填补了国内空白，在该领域境内市场“实现了进口替代”，获得了境内外全球顶级 PCB 客户的认可。 请发行人提供属于国家鼓励、支持和推动的关键设备、产品、零部件、材料并实现了进口替代的相关客观、支撑性政策文件、法律法规依据。 请发行人说明： （1）发行人提供了何种设备、产品、零部件、材料，是否属于国家鼓励、支持和推动的关键设备、产品、零部件、材料； （2）进口替代主要涉及的核心技术及应用情况，发行人在哪些方面、哪些领域实现了进口替代，进口替代的时间、程度，进口替代前后相关方面、领域的竞争情况、市场格局、内资外资及发行人的份额占比变化、发行人市场份额是否实现了部分外资替代，与境内外同行业可比公司在市场份额、销售额、市场地位、财务指标的对比情况； （3）进口替代相关的测试收入、净利润及占比、所涉及的主要客户等情况，发行人在价格、数量等相关方面的优势及销售占比的变化情况，发行人在市场竞争中的优劣势情况。 请发行人严格按照本所《科创板企业发行上市申报及推荐暂行规定》的要求细化披露相关信息；结合上述事项说明发行人是否符合《科创属性评价指引（试行）》《上海证券交易所科创板企业发行上市申报及推荐暂行规定》规定的科创属性及科创板定位。

以上就是笔者对相关案例的总结整理，以期为相关人工智能企业提供参考借鉴。

熊川
合伙人
资本市场部
上海办公室
+86 21 6085 3868
xiongchuan@zhonglun.com

人工智能与金融科技监管

作者/刘新宇、吴豪雳

2020全球人工智能大会上，中国人民银行科技司原司长陈静先生指出，人工智能应用很有希望将金融风险预警能力提高到崭新的水平，一定程度上说明了人工智能技术对金融科技发展的意义。作为新一轮科技革命和产业变革的重要驱动力量，人工智能技术与金融业的结合是金融科技发展的大势所趋，亦将显而易见地对未来的金融发展产生深远的影响。在金融科技实践中，人工智能技术已经在多个领域得到了较为普遍的运用，深入地参与到了金融行业的方方面面之中。同时，在金融科技领域，人工智能技术还往往与大数据、云计算、区块链等技术相结合，为金融业的发展提供了无限可能。

然而，我们也应该看到，在人工智能技术深刻影响金融变革的同时，人工智能技术的大规模运用亦在一定程度上影响既有的法律法规和金融秩序。例如，人工智能算法的不透明可能导致在自动化决策的过程中形成算法歧视，对消费者权益造成影响；再如大数据智能应用的广泛运用，可能带来数据安全和个人信息保护的相关问题。如何在运用人工智能技术服务金融创新和满足金融监管要求之间实现平衡，对于金融机构和金融科技企业而言，都是需要探索的问题。

PART 01

人工智能技术在金融科技领域的典型应用场景

当前，人工智能技术在金融科技的某些细分领域已经得到了较为普遍的运用，对金融业态的发展产生了全面、广泛的影响。就其中的典型应用场景，笔者试梳理如下：

（一）智能投顾

智能投顾，即指通过智能技术而开展的“投资顾问”业务，系根据现代资产组合理论，结合个人投资者的具体风险偏好与理财目标，通过后台算法为投资者提供的“投资顾问”服务。实践中，智能投顾业务开展过程中，智能投顾服务商一般首先通过大数据获得客户的个性化风险偏好、投资目标及其变化规律，并基于客户的个性化风险偏好，通过智能算法模型，定制出合理的个性化资产配置方案。之后，智能投顾还将利用互联网平台对客户的个性化资产配置方案进行动态实时的跟踪、调整与更新。

（二）算法交易

算法交易是金融科技领域最热门的技术之一，最早可追溯至上世纪70年代。它是指利用电子平台，输入包含算法的交易指令，以执行预先设定好的交易策略。在算法交易的应用场景下，算法决定交易下单的时机、价格乃至最终下单的数量与交易次数等。近年来，人工智能技术同算法交易的结合愈发紧密，越来越多的对冲基金、养老基金、投资机构等通过机器学习和深度学习，调整、优化算法，以采取更好的投资策略，提高资产收益。

（三）智能营销

传统金融机构的营销方式主要依赖于线下，智能化程度较低。随着人工智能技术的发展，众多科技巨头尝试将人工智能技术用于市场营销之中，结合机器学习技术，使用海量的标签进行模型的训练，以实现精准的营销，这正好迎合了金融机构数字化营销的需求。许多金融机构亦开始探索通过智能营销等方式建立以客户为中心的自动化营销平台，进行线上获客。

（四）智能风控

风控关系到金融机构的核心竞争力，是影响金融机构业务开展的重要环节，也是最广泛运用人工智能技术的金融场景之一。实践中，金融机构所开展的智能风控往往与大数据技术相结合，其基本逻辑一般是运用大数据平台的计算分析能力，机器学习或深度学习模型，并将相关模型运用于信贷风控、反欺诈、反洗钱、交易监控等具体场景。相较于传统的人工风控，智能风控更为稳定，有利于降低金融机构的风险管理成本。而对于一些风控能力相对较弱的中小金融机构来说，金融科技企业的智能风控技术亦可以作为风控能力建设的有效补充，对于金融机构业务开展具有重要作用。

（五）智能客服

近年来，金融机构对智能客服的需求逐渐提升。一方面，对于用户规模逐渐壮大的金融机构而言，其对客服人员数量的需求也相应地水涨船高，但盲目扩大客服队伍规模可能显著增加金融机构的人力成本，需要寻找成本相对可控的替代方案。另一方面，移动互联网的快速普及，让企业与客户的沟通变得多渠道的同时，也增加了用户对互动性的需求，需要企业寻求更加高效的客户沟通方式。基于此，智能客服逐渐为更多金融机构所采纳并使用。

PART 02

围绕人工智能技术的金融监管要求

（一）人工智能技术运用中的金融数据保护问题

实践中，人工智能技术在被用于金融科技场景时，往往同大数据技术相结合。由于金融业数据治理一直是金融监管部门关心的重点话题，故而在金融科技领域运用人工智能技术的过程之中，金融数据保护也是无法绕开的重点问题。

在智能风控、智能营销等场景下，往往涉及大量的数据处理，无论是金融机构，还是为金融机构提供金融科技服务的第三方，仅凭直接收集的数据一般难以满足业务需要，通过第三方数据供应商间接收集或采购数据已成为金融业务开展过程中的常态。在该过程中，若涉及的个人信息收集行为违反《中华人民共和国民法典》、《中华人民共和国网络安全法》的相关规定，则可能面临相应的法律责任。

近年来，金融行业业务分工愈发精细化，金融业务开展过程中可能涉及众多主体的共同参与。例如，针对一笔线上贷款业务，可能需要资金方、保险公司/担保公司、支付机构、征信机构、智能风控机构、助贷机构等多类机构参与其中，在该等场景下，数据的共享几乎不可避免。但由于共享过程中涉及到数据控制者的变更，如未能采取必要的措施对数据共享行为予以规制，导致数据被不当使用甚至数据泄露的发生，相关参与方均可能将因违反数据保护相关规定承担责任。

此外，在智能风控、智能投顾、智能营销等人工智能等应用场景中，金融机构可能依据算法等自动化决策手段作出决定，如基于用户画像决定个人信用及贷款额度等。对于该等信息系统自动决策行为，《中华人民共和国个人信息保护法（草案二次审议稿）》（以下简称“**《个保法（草案二审稿）》**”）第二十五条第一款亦提出了整体的规制要求，即应当保证决策的透明度和结果公平合理。同时，《个保法（草案二审稿）》第二十五条第二款、第三款针对自动化决策的特定场景提出了具体的要求，即对于通过自动化决策方式进行商业营销、信息推送的，应当同时提供不针对其个人特征的选项，或者向个人提供拒绝的方式；对于通过自动化决策方式作出对个人权益有重大影响的决定的，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。若后续《个保法（草案二审稿）》落地，则企业在使用相应人工智能应用时，应当确保符合上述规定，并为相关金融消费者提供相应救济途径。

（二）人工智能技术运用中涉及的金融营销宣传问题

如前所述，实践中，许多金融机构均将人工智能技术用于金融营销宣传之中，就该等营销宣传行为，一般还需要遵守金融营销宣传的相关规定。

例如，部分金融机构存在开展智能营销，向消费者手机推送金融营销宣传信息的行为。根据《关于进一步规范金融营销宣传行为的通知》，该等行为需要取得金融消费者同意。若未经金融消费者同意或请求，原则上不得以电子信息方式向其发送金融营销信息。即使取得了金融消费者的同意，金融机构在针对金融消费者开展金融营销宣传时，亦应当明确发送者的真实身份和联系方式，并向接收者提供拒绝继续接收的方式。

再如，部分金融营销信息可能通过互联网开展，该等金融营销信息可能以弹窗广告等形式呈现。若采用该等形式进行金融营销宣传的，应当显著标明关闭标志，确保一键关闭，并确保不影响他人正常使用互联网和移动终端。

（三）智能风控的特殊监管要求

智能风控是目前市场中头部金融机构和金融科技企业布局的重点，亦为人工智能技术在金融科技领域应用的重要表现。

1. “核心风控业务”不得外包

实践中，金融机构多将智能风控技术用于线上业务中。由于线上业务相对人往往分布在全国各地，部分中小金融机构尚不具备完全独立自主完成业务风险控制的技术能力。因而同提供智能风控服务的金融科技企业等第三方合作就成为了普遍现象。但在这个过程中，部分金融机构可能忽视了自身风控体系的建设，存在过分依赖甚至完全依赖外部智能风控技术的情形，催生了潜在的金融风险。

不可否认的是，大多数中小金融机构，在风控能力上确实同头部的互联网平台、金融科技企业存在一定的差距，因而在金融科技领域，寻求在智能风控方面的技术合作将是一种长期的趋势。值得引起关注的是，在这种长期合作中，金融机构仍应当对自身在智能风控各环节中的优缺点有充分的认识，有序引进和掌握各项数据资源和技术，尤其是实质性地做好信用评估、风险定价等核心环节的终审步骤。基于此，金融监管部门多次强调金融机构应当加强自身风控能力建设，严禁将授信审批、合同签订等核心风控业务外包。例如，在《关于规范整顿“现金贷”业务的通知》中，互联网金融风险专项整治工作领导小组办公室即要求“银行业金融机构与第三方机构合作开展贷款业务的，不得将授信审查、风险控制等核心业务外包。”《商业银行互联网贷款管理暂行办法》第八条第二款亦指出，“互联网贷款业务涉及合作机

构的，授信审批、合同签订等核心风控环节应当由商业银行独立有效开展。”此外，在针对银行卡、支付、小额贷款等多个领域的监管规定中，金融监管部门亦都强调了“核心风控业务不得外包”的要求。

2. 针对风控模型的特定监管要求

同时，风控模型往往囿于相对固定的算法，其能否在一定时间内长期提供可靠的风控服务亦存在不确定性，而风控模型的稳定与否关系到能否有效降低金融风险。以互联网贷款为例，监管部门在《商业银行互联网贷款管理暂行办法》中亦对风险模型管理提出了一定的监管要求，具体如下：

类别	具体要求	对应条文
权限配置	合理分配风险模型开发测试、评审、监测、退出等环节的职责和权限。	第三十七条
管理职责	不得将各环节风险模型的管理职责外包，并应当加强风险模型的保密管理。	
定制化要求	结合贷款产品特点、目标客户特征、风险数据和风险管理策略等因素构建模型，并进行正常测试和压力测试。	第三十八条
模型评审	建立风险模型评审机制，成立模型评审委员会负责风险模型评审工作，经评审通过后风险模型方可上线应用。	第三十九条
日常监测	建立有效的风险模型日常监测体系，监测至少包括已上线风险模型的有效性与稳定性，所有经模型审批通过贷款的实际违约情况等。监测发现模型缺陷或者已不符合模型设计目标的，应当保证能及时提示风险模型开发和测试部门或团队进行重新测试、优化，以保证风险模型持续适应风险管理要求。	第四十条
退出和处置	建立风险模型退出处置机制。无法继续满足风险管理要求的风险模型，应当立即停止使用，并及时采取相应措施，消除不利影响。	第四十一条
文档管理	全面记录风险模型开发至退出的全过程，并进行文档化归档和管理。	第四十二条

除以上风险模型管理相关规定外，《商业银行互联网贷款管理暂行办法》第二十二条亦要求，“商业银行应当建立人工复核验证机制，作为对风险模型自动审批的必要补充。商业银行应当明确人工复核验证的触发条件，合理设置人工复核验证的操作规程。”对于智能风控模型的运用而言，必要的人工复核验证既体现了对消费者权益的保护，也有助于金融机构根据实践变化及时对模型进行调整。

3. 智能风控与征信

实践中，智能风控公司在服务金融机构的过程中往往存在一并输出相应信用评价的情形。结合当前监管口径，该等输出信用评价的行为存在被认定为未经许可从事征信业务的风险。

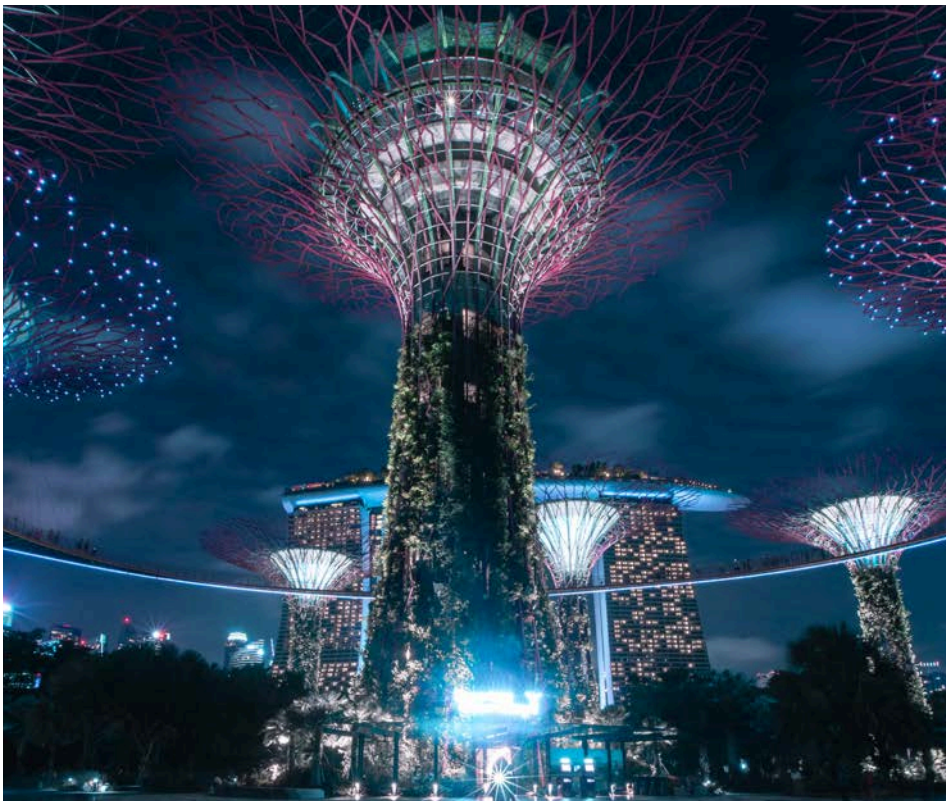
《征信业管理条例》第二条规定，“本条例所称征信业务，是指对企业、事业单位等组织的信用信息和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。”从该规定的文义出发，智能风控公司通过收集个人或企业的信用信息进行整理、加工，并向金融机构输出的行为基本符合征信业务的相关定义。结合近期要求网络平台实现个人信息与金融机构的全面“断直连”的监管口径，对于尚未取得个人征信牌照或完成企业征信备案的智能风控服务商，或应当尽快考虑取得相关资质。

（四）智能投顾的特殊监管要求

当前实践中，很多理财平台和基金销售平台，都已经将智能投顾技术运用到基金或理财产品的投资组合之中。但一方面，机构运用智能投顾技术服务的对象多为长尾客户，风险承受能力较低，如果投资者适当性管理不审慎、风险提示不到位，很容易引发不稳定事件。同时，若智能投顾技术大规模推广，算法的同质化可能加剧市场的波动，且算法自身具有一定的“黑箱”属性，监管机构和消费者均不易获悉投资决策的具体过程，也可能增加监管难度。基于此，就如何监管智能投顾技术的运用而言，境内监管部门在近年来也进行了一定的探索。

《关于规范金融机构资产管理业务的指导意见》（以下简称“**《资管新规》**”）在第二十三条针对智能投顾业务提出了一定的合规要求，明确“运用人工智能技术开展投资顾问业务应当取得投资顾问资质，非金融机构不得借助智能投资顾问超范围经营或者变相开展资产管理业务”，并要求开展智能投顾业务的机构仍应当履行投资者适当性、投资范围、信息披露、风险隔离等方面的一般性监管要求。

但对于《资管新规》所提到的“投资顾问”资质，目前仍尚未有明确落地



的规定予以规制。在前期试点的基础上，证监会于2020年4月发布了《证券基金投资咨询业务管理办法（征求意见稿）》，试就包括“证券投资顾问业务”和“基金投资顾问业务”在内的“证券基金投资咨询业务”进行规制，涵盖了资格条件、内部管理、业务规范、监管和法律责任等多个方面。该办法若正式落地，或有利于智能投顾业务在规范化的框架下进一步发展。

PART 03

金融机构与金融科技企业的应对措施

考虑到人工智能技术为金融科技的推广和金融业数字化转型的重要意义，其在金融行业的运用前景颇为广阔。但在将人工智能技术运用于各类金融科技场景的过程中，金融机构与金融科技企业亦应当采取必要的应对措施，确保符合相应的监管要求，避免潜在的法律风险。

具体而言，对于金融机构来说，在自主开发及运用人工智能技术的过程中，应当充分评估相关应用场景可能带来的潜在合规风险，遵守金融业务开展、金融数据保护、金融营销宣传等方面的相关监管要求。而在同第三方机

构开展人工智能领域相关合作的过程中，金融机构应当建立相应的供应商准入制度，对第三方机构的资质进行充分审查，并在合作协议中明确同第三方机构的权利义务分配。若第三方机构发生任何负面舆情或存在任何违法违规行为时，应当立即暂停相关合作，要求第三方机构说明相关情况，并在必要时终止合作，以避免相关风险向自身传递。

对于提供人工智能相关金融科技服务的企业而言，应当审慎评估自身业务模式，如拟开展的业务根据法律法规规定或监管要求需要持牌的，应当及时取得相应资质，以避免未经许可经营金融相关业务所带来的相关潜在风险。同时，其应当密切关注金融领域和金融科技领域的相关立法，尤其是关于金融业务资质、金融消费者权益保护的相关内容，及时根据法律法规规定调整业务模式，确保合法合规经营。

刘新宇
合伙人
私募基金与资管部
上海办公室
+86 21 6061 3700
jeffreyliu@zhonglun.com

人工智能在自动驾驶领域应用的法律问题

作者/丁恒、潘玲、金享、胡运思

在2021年7月8日至10日进行的2021世界人工智能大会中，有将近20家自动驾驶企业参加了大会。在全球受新冠肺炎疫情冲击的大背景下，人们的日常交往受限，自动驾驶却面临着前所未有的机遇——世界多国的自动驾驶技术和监管机制都取得了巨大的突破，尤其在中国，自动驾驶生态已经逐步建立完善。而人工智能作为自动驾驶领域中最重要和最复杂的组成部分，也迎来了巨大发展。

人工智能在自动驾驶技术中的应用最早可以追溯到2005年美国国防部高级研究计划局（DARPA）举办的无人驾驶车挑战赛，彼时由斯坦福大学Sebastian Thurn教授领导的无人驾驶汽车项目“Stanley”，使用传感器和一系列为无人驾驶车辆量身定制的算法软件，使得汽车本身可以寻找路径、探测并躲避障碍，最后成功通过了路况恶劣的赛道取得了胜利。Thurn教授后来加入了谷歌自动驾驶汽车项目，即后来为人熟知的Waymo。在此之后，人工智能在自动驾驶领域具有的突出优势越来越为人们所熟知，并且随着自动驾驶技术的发展，人们逐渐意识到自动驾驶车辆的上路运行无法或无法完全依赖人类驾驶员对于路况的感知与判断，当车体安装的雷达、摄像头等探测装置将收集到的交通数据传输至驾驶系统时，势必要依赖人工智能对这些数据进行实时传输、分析处理以及智能决策，因此将人工智能技术与无人驾驶技术的结合应用就水到渠成。总的来说，人工智能可以在环境感知、决策规划、控制执行三个应用场景[1]中为自动驾驶系统提供较为安全、稳定的支持，因而受到越来越多的自动驾驶技术开发者的关注，或者说高度自动驾驶技术的成熟和广泛应用必然要依靠人工智能。然而，人工智能运用到自动驾驶中，也会面临一系列的法律问题。本文将结合上述三个应用场景，从测绘、数据保护以及侵权责任的分配的角度分析人工智能在自动驾驶应用领域可能引起的法律问题。

1.《中国人工智能系列白皮书——智能驾驶》，中国人工智能协会，2017年10月。

PART 01

人工智能在自动驾驶领域应用的法律问题概述

1. 测绘问题

如前所述，人工智能可以在环境感知、决策规划、控制执行三个应用场景中为自动驾驶技术提供支持。在环境感知环节，人工智能技术会通过摄像头、雷达等传感器对周边的自然地理要素及地表人工设施等相关数据的采集及处理，以协助汽车作出正确的判断。而相关地理数据采集行为很有可能

被认定为《中国人民共和国测绘法》(以下简称"**《测绘法》**")中定义的测绘行为[2]。根据《测绘法》等相关规定,从事测绘活动的单位,应当依法取得测绘资质证书,并在测绘资质等级许可的专业类别和作业限制范围内从事测绘活动[3]。

根据《测绘资质管理办法》第二条及《关于加强自动驾驶地图生产测试与应用管理的通知》第一条,在测绘资质方面,自动驾驶企业可能需要取得的资质包括导航电子地图制作与互联网地图服务的相关资质。而关于导航电子地图制作,根据《外商投资准入特别管理措施(负面清单)(2020年版)》以及《外国的组织或者个人来华测绘管理暂行办法(2019年修正)》的相关规定,导航电子地图制作属于禁止外商投资的项目;关于互联网地图服务,外国投资者也需要与中国企业采取合资、合作的形式来开展该等业务。

实践中,考虑到测绘资质对于外资背景的限制以及测绘资质本身申请难度较高[4],对于自动驾驶企业来说,其往往会选择与拥有相应测绘资质的企业进行合作,让具有测绘资质的企业对相应地理数据进行采集和处理,自己仅负责提供自动驾驶方案,以此形式开展业务。通过这种模式,笔者认为可以无需取得相关测绘资质。反之,如果自动驾驶企业将自动驾驶过程中采集的相关数据先传输到自动驾驶企业,再由自动驾驶企业传输至地图制作单位的,那么自动驾驶企业在此过程中的行为就很有可能被认定为测绘行为。

目前,随着人工智能技术的不断发展,导航电子地图的制作技术也在不断发展。这些发展,将直接影响自动驾驶企业在测绘行为中所起到的作用,进而进一步影响自动驾驶企业的测绘资质获取问题。关于此问题,笔者认为需持续关注最新的立法动态。

2. 数据保护问题

在自动驾驶情境下,在环境感知、决策规划、控制执行三个应用场景中,均存在数据收集、数据交换和数据处理的相关行为。目前,以欧盟《通用数据保护条例》("**GDPR**")为代表,世界主流国家都在加快个人信息保护法律的制定,并对数据的收集、使用和传输进行规制。一般来说,对于自动驾驶情境下的数据规制,主要以各国的网络安全和个人信息保护规定为主,辅以针对汽车行业数据的特别规定。下文以中国相关规定为例,进行详细分析。

①数据收集需要注意的事项

依靠机器的深度学习、对数据进行分析处理是人工智能自动驾驶汽车成功的基础[5],而机器的深度学习离不开大量的数据训练,因此人工智能自动驾驶将可能引发大量对于个人信息以及交通道路数据等数据的收集。自动

2.《测绘法》第二条第二款,本法所称测绘,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。

3.《测绘资质管理办法》第一条。

4.关于测绘资质,根据《测绘资质管理办法》和《测绘资质分类分级标准》导航电子地图制作的乙级资质需要具有15名专业人员、外业数据采集设备5台(套)(定位精度≤10m)并且仅可在相关政府部门划定的自动驾驶区域内从事导航电子地图制作,而若要取得甲级测绘资质则要满足拥有不少于100名的专业人员、外业数据采集设备30台(套)(定位精度≤10m)。互联网地图服务的乙级资质不得从事地图数据开发,并且需要拥有12名的专业技术人员,而甲级测绘资质则需要拥有20名专业技术人员以及独立地图引擎。

5.《详述人工智能在自动驾驶中的应用》,智车科技,访问地址:https://blog.csdn.net/datawhale/article/details/114558118?utm_term=%E4%BA%BA%E5%B7%A5%E6%99%BA%E8%83%BD%E5%9C%A8%E8%87%AA%E5%8A%A8%E9%A9%BE%E9%A9%B6%E4%B8%AD%E7%9A%84%E5%BA%94%E7%94%A8&utm_medium=distribute.pc_aggpage_search_result.none-task-blog-2~all~sobaiduweb~default-0-114558118&spm=3001.4430,最后访问时间:2021年7月6日。

驾驶服务商不仅可能是汽车实体的制造者，通常情况下，它还是车联网服务的提供者和实际管理者，向自动驾驶用户提供网络服务。因此，自动驾驶服务商实际上扮演了《网络安全法》（以下简称"**《网安法》**"）项下所定义的"网络运营者[6]"的角色。不仅如此，由于自动驾驶所在的交通行业属于《网安法》第三十一条所规定的"重点行业"，国家实行重点保护，结合《关键信息基础设施安全保护条例（征求意见稿）》第十八条[7]对于关键信息基础设施的具体定义，笔者理解，自动驾驶服务商极有可能被认定为关键信息基础设施的运营者（即Critical Information Infrastructure Operators "**CIIO**"）[8]。对于CIIO，在中国网络安全和数据合规监管体系下，对其有着相对于一般网络运营者更高的合规标准。

笔者认为，自动驾驶服务商的个人信息收集应特别关注以下两个方面：

◆在信息收集的范围上，需要符合汽车数据安全监管的要求以及对汽车行业重要数据的特殊规定。

◆在信息收集的过程中，需要考虑隐私政策与用户同意的合规性。

在数据收集的范围上，除了遵循最小必要原则进行用户信息收集，根据2021年6月10日通过的《数据安全法》的相关规定，自动驾驶服务商需要甄别其收集使用的信息是否属于汽车行业的"重要数据"，并对"重要数据"进行重点保护。在国家网信办于2021年5月12日发布的《汽车数据安全管理若干规定（征求意见稿）》（以下简称"**《汽车数据规定》**"）中，规定了汽车数据收集的"默认不收集"原则，并对汽车行业的重要数据进行了明确，规定了6类重要数据，分别为重要敏感区域的人流车流数据、高精地图测绘数据、汽车充电网的运行数据、道路车辆类型、流量等数据、道路车辆类型，流量等数据、包含人脸，声音，车牌等车外音视频数据以及其他可能影响国家安全，公共利益的数据。[9]。处理该等数据，需要依照《汽车数据规定》下的重要数据处理原则进行处理，如车内处理、非必要不向车外提供以及数据本地化要求等。笔者建议自动驾驶服务商在收集数据时，依照国家相关法律法规，对数据进行甄别并分类，并依据数据的类型采取不同的措施。

在数据收集的过程中，自动驾驶车辆与驾驶员之间的互动通常是通过驾驶员的智能移动设备实现的[10]，而车载用户交互软件的设计和使用，通常涉及到用户隐私政策的编写。隐私政策与用户的知情、同意、撤回同意以及拒绝权息息相关。通常做法是自动驾驶服务商将需要向用户明示告知的所有有关数据收集、处理、传输的重要信息纳入隐私政策，从而使得用户能够及时、充分地了解自己数据的收集处理情况，以方便用户行使同意、撤回同意或拒绝信息收集、使用和传输的权利。在中国，根据《网安法》及国家标准

6.根据《网安法》第七十六条，网络运营者，是指网络的所有者、管理者和网络服务提供者。实践中，对网络运营者的解释非常宽泛。

7.《关键信息基础设施安全保护条例（征求意见稿）》第十八条：下列单位运行、管理的网络设施和信息系统，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，应当纳入关键信息基础设施保护范围：（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位…

8.《网络安全法》第三十一条。

9.《汽车数据安全管理若干规定（征求意见稿）》第三条。

10.《自动驾驶汽车开发注重数据合规性》，北京市高级别自动驾驶示范区，访问地址：https://mp.weixin.qq.com/s/LDh1yAJHxkGi1R_84wmmcg，最后访问时间2021年6月29日。

《GB/T 35273-2020 信息技术安全 个人信息规范》（以下简称“**《个人信息规范》**”）等相关法律法规要求，个人信息保护政策应清晰、准确、完整地描述个人信息控制者的个人信息处理行为。因此对于自动驾驶服务商而言，在设置汽车人机交互系统时，应当确保隐私政策中，对于信息的处理作出了较为全面和清晰的说明，且内容对于用户而言通俗易懂，以此获得用户基于充分了解信息收集、处理规则作出的明确、清楚的同意。

② 个人数据处理需要注意的事项

笔者理解，在自动驾驶场景下，人工智能系统会对用户日常驾驶爱好进行收集分析，从而形成下一次入舱时的默认设定；不仅如此，系统可能还会基于驾驶员的驾驶习惯，在突发事件下对汽车的运行方案作出指示。而这些操作，很大程度上依赖于对用户画像进行数据处理。用户画像在许多国家的数据保护法中都受到严格的限制，原因在于用户画像涉及到机器对人进行评价、分类，从而进行倾向性判断。用户画像的下一步通常是自动化决策，由于自动化决策存在对于决策对象的性别、肤色、宗教、种族等歧视的风险，因此各国对于这类技术的运用一直比较谨慎。

在我国，用户画像并不被绝对禁止。根据《个人信息规范》第7.4条的规定，使用用户画像时，个人信息控制者除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。笔者理解，当数据主体明示授权可以对其进行用户画像，以完成驾驶任务、优化驾驶体验时，用户画像是被允许的。但是需要注意的是，如果用户画像可能会引起自动化决策，那么在决策时要注意用户画像的合规性，比如该种自动化决策是否真的有必要。在紧急情况下，自动驾驶汽车该牺牲哪方利益、保护哪方利益（例如，在对人类生命安全造成损害无可避免时，应当牺牲和挽救哪类人群的利益）在伦理上都一直存在争议，这时驾驶系统的自动化决策应当更加审慎，从而降低争议的风险。

③ 数据出境需要注意的事项

由于相当一部分自动驾驶企业涉及到跨国业务，许多自动驾驶企业出于监管或商业等因素的考量，选择将自己的数据储存在国外的服务器上，从而不可避免地产生跨境数据流。随着各国对于跨境数据传输提出越来越高的合规要求，自动驾驶企业势必需要关注不同国家和地区的跨境数据传输规则。

如前文所述，在中国《网安法》项下，作为网络运营者及CIIO，自动驾驶服务商在数据出境方面，需要特别谨慎，比如应以数据本地储存为原则，仅在特殊情况下可以出境，且数据出境必须进行安全评估[11]。

11.根据国家标准化管理委员会发布的《信息安全技术 数据出境安全评估指南（征求意见稿）》，作为关键信息基础设施运营者的自动驾驶服务商，其数据出境会触发国家网信部门、行业主管部门启动主动评估的条件。

值得一提的是，面对各国不同标准的数据保护法，自动驾驶汽车企业还可能面临需要在各国分别合规的复杂情况。如今各国数据保护标准和体系参差不一，各国数据保护法在数据的范围、保护规则和惩罚力度等方面都有着相当显著的差异。这也为自动驾驶汽车企业在业务中较难避免的跨境数据流动设置了障碍。

3. 侵权责任

相较于传统交通事故，自动驾驶涉及的主体包括自动驾驶汽车生产商、自动驾驶服务商、汽车销售者、车辆使用人、车辆驾驶员等。自动驾驶模式下由于侵权涉及主体的多元化，导致了侵权行为和损害后果之间的因果关系更为模糊，传统的机动车交通事故责任的归责原则逐渐受到挑战。在此情形下，当自动驾驶车辆发生事故并造成人员伤亡或财产损失时，如何在人类驾驶员和自动驾驶系统（或者说，自动驾驶系统的最终责任人）之间判定责任就成为了问题的核心。鉴于目前主流的自动驾驶技术以3级驾驶自动化（有条件自动驾驶）[12]，即人机混合驾驶模式为主，以下，笔者将以3级驾驶自动化模式为例，对此问题进行简要论述。

①驾驶人责任

关于处于3级驾驶自动化状态下的汽车发生交通事故，驾驶人是否应当承担侵权责任的问题，笔者认为，首先应当判断在3级驾驶自动化状态下驾驶人对车辆是否负有管理义务。

根据国家推荐性标准《汽车驾驶自动化分级（推荐性国家标准报批稿）》3.5.4条[13]，3级驾驶自动化状态下，驾驶人需要在车辆发出接管请求或者车辆处于不适合自动驾驶的状态时接管车辆。《深圳经济特区智能网联汽车管理条例（征求意见稿）》第二十六条[14]，也有类似规定。

因此，笔者认为，对于3级驾驶自动化状态下的汽车，驾驶员依然负有管理汽车的义务，需要识别车辆是否满足设计运行条件，并在车辆发出接管请求时立即接管汽车。不仅如此，自动驾驶汽车的驾驶员还负有对车辆进行维修、保养，对人工智能系统、导航地图等及时进行更新的义务。

根据传统的机动车交通事故责任的归责原则[15]，机动车之间发生交通事故采用过错归责原则，按照各自过错的比例分担责任。机动车与非机动车驾驶人、行人之间发生交通事故的，双方均无过错时采用无过错归责原则，由机动车驾驶人承担侵权责任，非机动车驾驶人、行人有过错的可适当减轻机动车一方的责任。

因此，笔者认为，鉴于在3级驾驶自动化状态下，驾驶员依然负有管理汽

12.根据《汽车驾驶自动化分级（推荐性国家标准报批稿）》，驾驶自动化可以分为五级，分别为0级驾驶自动化（应急辅助）、1级驾驶自动化（部分驾驶辅助）、2级驾驶自动化（组合驾驶辅助）、3级驾驶自动化（有条件自动驾驶）、4级驾驶自动化（高度自动驾驶）、5级驾驶自动化（完全自动驾驶）。其中，3级驾驶自动化（有条件自动驾驶）是指驾驶自动化系统在其设计运行条件内持续地执行全部动态驾驶任务。对于3级驾驶自动化，动态驾驶任务接管用户以适当的方式执行动态驾驶任务接管。

13.3级驾驶自动化系统应满足以下要求：a）仅允许在设计运行条件内激活；b）激活后在设计运行条件内执行全部动态驾驶任务；c）识别是否即将不满足设计运行条件，并在即将不满足设计运行条件时，及时向动态驾驶任务接管用户发出接管请求；d）识别驾驶自动化系统失效，并在发生驾驶自动化系统失效时，及时向动态驾驶任务接管用户发出接管请求；e）识别动态驾驶任务接管用户的接管能力，并在用户的接管能力即将不满足要求时，发出接管请求；f）在发出接管请求后，继续执行动态驾驶任务一定的时间供动态驾驶任务接管用户接管；g）在发出接管请求后，如果动态驾驶任务接管用户未响应，适时执行风险减缓策略；h）当用户请求驾驶自动化系统退出时，立即解除系统控制权。

14.《深圳经济特区智能网联汽车管理条例（征求意见稿）》第二十六条，驾驶人应当在车辆发出接管请求或者车辆处于不适合自动驾驶的状态时立即接管智能网联汽车。

15.《民法典》第一千二百一十三条，机动车发生交通事故造成损害，属于该机动车一方责任的，先由承保机动车强制保险的保险人在强制保险责任限额范围内予以赔偿；不足部分，由承保机动车商业保险的保险人按照保险合同的约定予以赔偿；仍然不足或者没有投保机

车的义务，当自动驾驶车辆的驾驶人在未尽到上述义务与机动车发生交通事故时，应当根据其过错程度承担相应责任，与非机动车驾驶人、行人之间发生交通事故时，则无论是否有过错均应承担相应责任。

② 生产者产品责任

自动驾驶汽车的生产者包括人工智能系统生产者与传统机械载体生产者。由于传统机械载体生产者责任与非自动驾驶汽车并无不同，限于篇幅，本文不再赘述，以下仅分析人工智能系统生产者的产品责任。

根据《产品质量法》第四十六条，“本法所称缺陷，是指产品存在危及人身、他人财产安全的不合理的危险。”从产品缺陷存在的和合理性角度出发，可将人工智能系统的产品缺陷分为可控缺陷与不可控缺陷。

首先，关于人工智能系统的可控缺陷目前主要包括：①系统本身的设计缺陷、②对驾驶人发出接管请求的示警系统的缺陷等。此类可控缺陷的特点在于生产者可以在源头上控制风险，通过技术升级、预置算法等规范生产者的行为可大大降低风险发生的可能。因此，笔者认为，此类可控缺陷应依据《民法典》以及《产品责任法》的相关规定[16]，由生产者和销售者承担不真正的连带责任。

其次，关于人工智能系统生产者的不可控缺陷包括：通过人工智能的自主深度学习，以及与周围环境的相互作用，基于人工智能系统独立判断产生的缺陷。由于此类缺陷的高度不可预测性，将此类责任归责于生产者将大大打击各大人工智能企业的研发积极性。因此，笔者认为，与其讨论如何归责，不如设立一套完备的生产者风险转移制度，如自动驾驶汽车强制责任险制度，强制要求自动驾驶企业为其产品进行投保，以兼顾产业发展与受害者救济之间的平衡。

总结

由于人工智能够在环境感知、决策规划、控制执行等环节为驾驶系统提供极大的便利，随着科技的发展和成本的降低，人工智能在自动驾驶的应用将趋向普及化。而随着人工智能在自动驾驶系统中扮演越来越重要的角色，它的风险也逐渐显现：在测绘方面，根据自动驾驶企业在数据采集的过程中起到的作用，涉及到自动驾驶企业可能需要应对相关测绘资质的取得问题；在数据安全方面，自动驾驶企业在个人信息及交通道路等数据的收集、使用和传输等方面都可能面临着向不同数据主体进行合规性应对的风险。此外，由于自动驾驶数据可能包含《网络安全法》和《数据安全法》定义下的重要数据和敏感数据，相对应地，可能面临着更高的合规要求；在跨境数据流动方

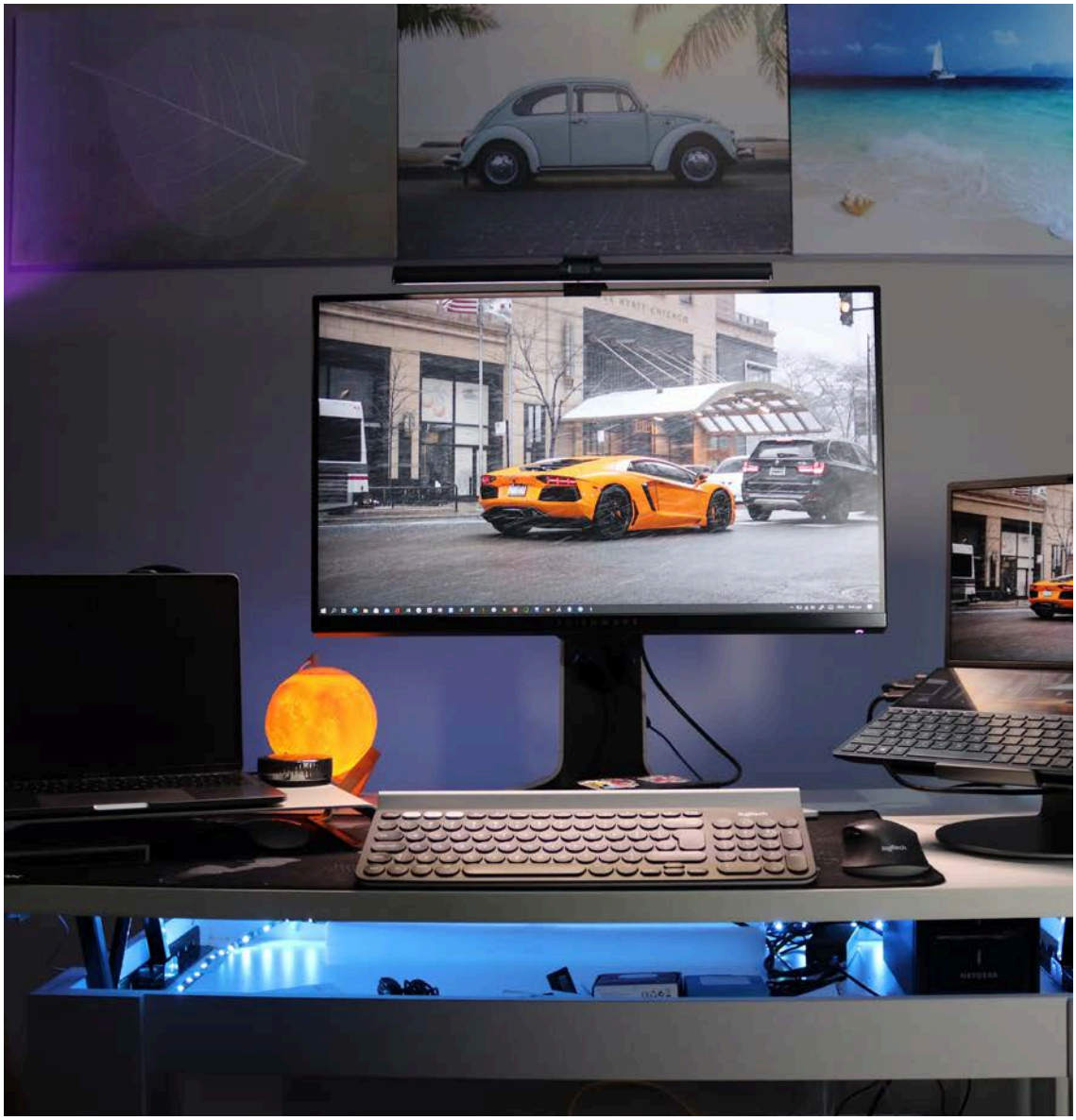
动车商业保险的，由侵权人赔偿。
《道路交通安全法》第七十六条，机动车发生交通事故造成人身伤亡、财产损失的，由保险公司在机动车第三者责任强制保险责任限额范围内予以赔偿；不足的部分，按照下列规定承担赔偿责任：（一）机动车之间发生交通事故的，由有过错的一方承担赔偿责任；双方都有过错的，按照各自过错的比例分担责任。（二）机动车与非机动车驾驶人、行人之间发生交通事故，非机动车驾驶人、行人没有过错的，由机动车一方承担赔偿责任；有证据证明非机动车驾驶人、行人有过错的，根据过错程度适当减轻机动车一方的赔偿责任；机动车一方没有过错的，承担不超过百分之十的赔偿责任。

16.《民法典》第一千二百零三条，因产品存在缺陷造成他人损害的，被侵权人可以向产品的生产者请求赔偿，也可以向产品的销售者请求赔偿。产品缺陷由生产者造成的，销售者赔偿后，有权向生产者追偿。因销售者的过错使产品存在缺陷的，生产者赔偿后，有权向销售者追偿。
《产品责任法》第四十一条，因产品存在缺陷造成人身、缺陷产品以外的其他财产（以下简称他人财产）损害的，生产者应当承担赔偿责任。
生产者能够证明有下列情形之一的，不承担赔偿责任：（一）未将产品投入流通的；（二）产品投入流通时，引起损害的缺陷尚不存在的；（三）将产品投入流通时的科学技术水平尚不能发现缺陷的存在的。
《产品责任法》第四十三条，因产品存在缺陷造成人身、他人财产损害的，受害人可以向产品的生产者要求赔偿，也可以向产品的销售者要求赔偿。属于产品的生产者的责任，产品的销售者赔偿的，产品的销售者有权向产品的生产者追偿。属于产品的销售者的责任，产品的生产者赔偿的，产品的生产者有权向产品的销售者追偿。

面，自动驾驶企业除需要符合中国法项下的相关合规要求，还需要考虑数据接收国以及数据流可能经过的国家和地区的数据保护规则；在侵权责任分配方面，在事故发生时，在目前主流的自动驾驶技术项下，仍需要人类驾驶员依过错承担责任；而对于相关产品责任，笔者认为，人工智能系统生产者应与销售者承担不真正连带责任。

当然，由于人工智能技术所引导的自动驾驶的新颖性，目前法律对于这一新技术应用所可能产生的许多问题尚有待明确之处，笔者认为还需在未来，结合实际中产生的具体问题进行进一步讨论。

丁恒
合伙人
公司业务部
上海办公室
+86 21 6061 3736
dingheng@zhonglun.com



人工智能应用场景中GDPR下车联网数据风险及应对
——解读EDPB《车联网个人数据保护指南》

作者/陈际红、韩璐、杨润

2020年8月5日，国家标准化管理委员会、中央网信办、国家发展改革委、科技部及工业和信息化部联合印发了《国家新一代人工智能标准体系建设指南》，其中明确指出："注重人工智能与车联网等相关标准体系的协调配套。充分发挥标准对产业发展的支撑引领作用，为高质量发展保驾护航。"而随着车联网技术的不断发展，联网车辆也逐渐进入主流市场，传统汽车制造商纷纷进行数字化转型，发展人工智能相关车联网技术，与众多传统汽车行业和新兴数字经济行业参与者共同构建起车联网的人工智能生态系统。由于车联网生态系统的复杂性以及在此过程中参与各方针对个人数据的处理活动互联的紧密性，所引发的个人数据保护问题受社会各界的广泛关注。

在《通用数据保护条例》(General Data Protection Regulation, 以下简称为"**GDPR**")规范的个人数据保护框架下，2020年1月28日，欧盟数据保护委员会(European Data Protection Board，**EDPB**)发布了《在联网车辆和出行相关环境下处理个人数据的指南(公开征求意见稿)》(以下简称为"**《车联网个人数据保护指南》**")(Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications - version for public consultation[1])，较为明确地阐释了车联网应用环境下的个人数据处理活动中存在的隐私和数据保护风险并相应提出了应对措施，对车联网行业参与各方具有重要的借鉴意义。

1.https://edpb.europa.eu-/our-work-tools/-public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en，最后访问时间：2020年6月3日。

2. 车载T-BOX又称车载通信终端，主要用于和后台系统/手机APP通信，实现手机APP的车辆信息显示与控制。

PART 01
车联网应用环境下的个人数据

在出行管理、车辆管理、道路安全、娱乐、驾驶员辅助、健康检测等各类复杂的车联网应用环境下，无论车辆本身联网或者未联网，个人数据均可通过车辆传感器、车载T-BOX[2](telematics box)或者手机应用(例如与车内系统连接的驾驶员手机)等被收集。

传统意义上单纯与车辆相关的数据可能不会构成个人数据，但是在车联网应用环境下，与联网车辆交互所产生的大部分数据可以通过人工智能识别等方式，锁定到特定的自然人或与识别自然人有关，因此可构成GDPR下的个人数据。其中既包括可直接识别自然人的数据，例如车主或驾驶员的身份信息；也包括可间接识别自然人的数据，例如行使里程等车辆使用行为数据、车辆零部件磨损相关数据等车辆的技术数据。此类数据与其他信息【特别是车辆识别号(Vehicle Identification Number，**VIN**)】相关联即可

识别到特定自然人。

具体而言，适用于《车联网个人数据保护指南》的个人数据主要包括：车主、驾驶员、乘客、承租人等个人数据主体的①在车内处理的个人数据；②车辆和与之相连的设备（例如车主、驾驶员或乘客的智能手机）之间交换的个人数据；以及③在车内收集并为进一步处理而向外部实体（如汽车制造商、保险公司、汽车维修商等）输出的个人数据。同时，《车联网个人数据保护指南》亦明确车联网应用环境下基于雇佣关系产生的个人数据、车辆内置WiFi相关的个人数据以及协同智能驾驶系统（Cooperative Intelligent Transport Systems，C-ITS）相关的个人数据由于其特殊性，不适用于该指南。

PART 02
车联网应用环境下的个人数据处理风险

在车联网应用环境下的个人数据处理活动中，涉及的参与各方可能包括汽车制造商、设备制造商、汽车零部件供应商、汽车维修商、汽车经销商、汽车租赁/共享公司、保险公司、娱乐提供商、电信运营商、道路基础设施管理方和公共部门等。鉴于参与各方在车联网生态系统中所处的交互环节、角色的不同，所面临的个人数据保护风险也有所不同。《车联网个人数据保护指南》概括了以下几种车联网应用环境个人数据处理活动的典型风险：

1. 个人数据主体对其个人数据缺乏控制以及信息不对称

一方面，个人数据处理活动的相关信息可能仅为车主所知悉（例如在车主购车时向其提供隐私政策或者购车协议中规定的相关内容），驾驶员和乘客可能并未被告知此类信息，导致真正受影响的个人数据主体对其个人数据的控制权不足。

另一方面，由于人工智能与车联网技术的复杂性，个人数据主体不可能完全清楚地理解其个人数据被处理的具体情况，导致在个人数据主体可能没有意识到的情况下，其个人数据即被人工智能默认或自动触发相关收集和处理活动。

2. 个人数据主体做出的同意可能无效

根据欧盟委员会《电子隐私指令》（ePrivacy Directive），在用户终端设备中存储信息、访问已经存储的信息必须取得个人数据主体的事先同意[3]，且该条规定优先于GDPR第6条关于法律基础的规定适用[4]。在车联网应用环

3.Directive 2002/58/EC of the European Parliament and of the Council Directive on privacy and electronic communications (ePrivacy Directive) Article 5 (3): Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

4.EDPB《5/2019 关于<电子隐私指令>和GDPR相互作用的意见》(Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019)

境下，联网车辆和任何一个与其相连的设备均会构成一个终端设备，因此在此类终端设备中存储和访问数据应当事先征得个人数据主体的同意。

根据WP29关于同意的解释指南【以及EDPB在《车联网个人数据指南》之后所发布的《对第2016/679号条例下同意的解释指南》（Guidelines 05/2020 on consent under Regulation 2016/679[5]）】，同意应当同时满足自愿做出、具体、知情、明示的意思表示及可随时撤回和数据控制者可证明的要求方可有效[6]。在车联网，特别是人工智能应用环境下，个人数据主体甚至可能注意不到车内在进行的数据处理活动，无法做出建立在知情基础上的同意；其次，在实践中普遍存在的二手车买卖、租车等情况下，驾驶员及乘客与车主之间无直接联系，更加难以获得直接受影响的个人数据主体（即驾驶员及乘客）的同意。

3. 对个人数据的进一步处理可能缺乏相应的法律基础

就个人数据的处理活动而言，参与各方对个人数据进行的处理活动时应当严格遵循目的限制及最小化原则的要求，仅在收集个人数据时所明确的目的范围内进行处理活动。若参与各方需对个人数据进一步处理，此时新的处理活动无法与原目的兼容，则应当具备新的法律基础。举例来说，汽车维修商基于车辆维修目的所收集的遥测数据，不应在未获驾驶员同意向其提供基于驾驶行为的保险单的情况下，向机动车保险公司披露。

就配合执法机构的执法活动而言，当满足特定条件时，执法机构可能会处理联网车辆所收集的数据来探测超速或其他违法行为。需要注意的是，EDPB指出，仅为满足执法机构的要求而进行的个人数据处理不构成GDPR第5条意义上的“特定、明确和合法的目的”，仅在执法机构经过法律授权成为GDPR项下的“第三方[7]”时，车辆制造商可以根据各成员国的具体法律规定向执法机构提供个人数据主体的相关数据。

4. 个人数据的过度收集

在车联网应用环境下，由于联网车辆技术及人工智能技术本身的复杂性及前沿性，一方面装配到联网车辆上的传感器数量不断增加，导致需收集的数据规模更大，类型更加复杂，从而引发过度收集个人数据的风险；另一方面基于机器学习算法的人工智能联网车辆在功能开发时可能需要长期收集大量数据以进行深度学习，天然地存在过度收集个人数据的风险。

5.https://edpb.europa.eu-/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en，最后访问时间：2020年6月1日。

6.WP29《对第2016/679号条例（GDPR）下同意的解释指南》（Article 29 Working Party Guidelines on consent under Regulation 2016/679）

7.根据GDPR第4条第（10）项，“第三方”指的是除了数据主体、控制者、处理者、控制者或处理者直接授权其处理个人数据之外的自然人或法人、公共机构或组织。

5. 个人数据的安全风险较高

由于车联网系统本身的关键性以及应用环境中自然人的高度参与，一旦发生个人数据安全事件，有极大的可能会危及到个人的生理健康和生命安全，造成对自然人重大利益的损害。

联网车辆所面临的安全风险主要来自于两个方面：首先是联网车辆所提供的多元功能、服务及界面增加了其遭受网络安全攻击的可能性；其次是对于存储在车辆上或者诸如云服务器等外部环境中的个人数据，可能无法完全保证其已得到充分的安全保障。

PART 03

人工智能与车联网应用环境下的个人数据处理风险应对

为充分控制车联网应用环境下的个人数据处理风险，避免损害个人数据主体的基本权利、自由及公共利益，《车联网个人数据保护指南》针对上述典型风险提出了基本的应对建议，为参与各方在车辆网应用环境下进行个人数据处理活动提供了充分参考。

1. 三类重点关注的个人数据

只要可能关联到一个或多个可识别的自然人，大多数与联网车辆相关的数据将被视为个人数据。EDPB认为参与各方应当重点关注以下三类个人数据：位置数据、生物识别数据以及可揭露犯罪行为或交通违法行为数据。

对于地理位置数据的收集和使用，参与各方应当遵守以下原则：

①充分评估收集的频率、细节程度等。（例如，避免过度收集个人数据，即使获得了数据主体的同意，天气应用也不应当以每秒一次的收集频率访问车辆的地理位置数据）；

②充分告知个人数据主体针对其位置数据进行处理的详细信息；

③若收集、处理位置数据的活动需以个人数据主体的同意作为法律基础，应当征得其有效同意；

④仅当个人数据主体要求启动必需获取车辆地理位置的功能时，方可激活地理位置的收集，不可在车辆启动时以默认和持续的方式启动收集行为，同时应当为个人数据主体提供可随时禁用地理位置的选项；

⑤以图标等明显的方式告知个人数据主体地理位置已被激活。

对于生物识别数据的收集和使用，首先，参与各方应当为个人数据主体提供不需要收集生物识别的替代方案，且不会向个人数据主体施加额外的

约束条件；其次，参与各方在收集生物识别数据后，应当通过以下方式充分保障数据的安全：①仅在本地以加密形式存储和比对生物识别模板，确保生物识别数据不会被外部的读取/对比终端处理；②确保所使用的生物识别传感器及解决方案具备充分的安全能力；③避免存储原始数据，对构成生物识别模板和用于用户验证的原始数据进行实时处理。

对于可揭露犯罪行为或交通违法的数据的收集和使用，EDPB建议参与各方采取本地处理的方式，确保个人数据主体对所涉数据具有完全的控制权，同时保护数据免于非法访问、修改和删除。除某些特殊的例外情形，禁止参与各方对可揭露犯罪行为或交通违法的数据进行外部处理。

2. 严格遵循目的限制原则及数据最小化原则

根据GDPR，个人数据处理的目的应当是特定、明确和合法的，每一种处理活动均应具备相应的法律基础，同时个人数据处理活动应当仅在实现目的所必需的范围内进行。为充分遵守目的限制原则及数据最小化原则，在收集个人数据时，参与各方应当特别注意所收集的与联网车辆相关的个人数据类型，确保仅收集与处理相关和必要的、最小范围内的个人数据；在使用个人数据时，参与各方应当确保仅在收集个人数据时所明确的目的范围内进行使用，对个人数据的处理、存储应当仅限于实现该特定目的所必要的期限内。

3. 实现设计和默认的数据保护

设计和默认的数据保护（Protection by Design and by Default，**PbD**）是指在任何系统、服务、产品或流程的设计阶段以及全生命周期中充分考虑数据保护问题，同时确保在默认情况下仅处理目的所需的个人数据。

《车联网个人数据保护指南》中提出了可供车联网应用环境下的参与各方参考的通用实践，参与各方应尽量做到：

①尽量采取本地处理的方式，保证个人数据主体对其个人数据的控制权。同时可考虑开发车载应用平台，对与安全相关的相应功能进行物理分离，避免依赖不必要的外部云能力；

②如果数据必须传输至车辆以外，应当在传输之前对个人数据进行匿名化处理；

③考虑到车联网应用环境下的个人数据规模和敏感性，处理个人数据（尤其是在车辆外部进行处理的情况下）可能会给数据主体的权利和自由带来高风险[8]。在这种情况下，建议参与各方进行个人数据保护影响评估（Data

8.根据GDPR第35条及第29工作组于2017年发布的《关于2016/679条例下DPIA及判断数据处理活动时候会造成高风险的指南》（Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679），当数据处理活动可能会给自然人基本权利和自由带来高风险时，应当在处理个人数据之前进行DPIA。必须进行DPIA的典型情形包括：(a) 以自动化决策（包括用户画像）为基础对数据主体进行系统性与全面性的评价，作出对其产生法律影响或其他类似重大影响的决定；(b) 以大规模的方式处理特殊类别个人数据或与刑事犯罪、定罪相关的数据；(c) 以大规模的方式系统性地对公众可访问的空间进行监控。

9.笔者注：关于该指南的详细解读，可参考《他山之石：EDPB<关于GDPR第25条设计和默认的数据保护指南>（上）（下）》，http://www.zhonglun.com/Content/2019/12-25/1544107653.html；http://www.zhonglun.com/Content/2019/12-26/1909462215.html.

Protection Impact Assessment, **DPIA**），在推出新技术之前将风险分析的结果纳入设计过程。

EDPB于2019年11月13日所发布的《关于GDPR第25条设计和默认的数据保护指南（公开征求意见稿）》（Guidelines 4/2019 on Article 25 Data Protection by Design and by Default，version for public consultation）全面地介绍了实现设计和默认的数据保护的具体措施[9]。

4. 保障个人数据主体权利

保障个人数据主体权利，参与各方一方面需要在处理个人数据之前充分告知数据主体关于数据控制者的具体身份、处理目的、数据接收方、数据存储期限以及数据主体所享有的权利等详细信息。在间接收集的场景下（例如，车辆制造商可能会依靠经销商来收集数据主体的个人数据以便提供紧急路边援助等服务），上述信息可通过车辆销售合同、服务合同等书面文件或车载显示屏展示的条款告知个人数据主体。

另一方面，参与各方应当为个人数据主体提供可实现其权利的途径，促

进个人数据主体在整个处理过程中对其个人数据的控制的权利实现。为了便于个人数据主体对设置进行修改，车辆制造商可以考虑在车辆内部安装用户配置文件管理系统。

10.http://www.gov.cn/zhengce/zhengceku/2020-02/24/content_5482655.htm，最后访问日期：2020年6月3日。

5. 加强数据安全保障

为充分控制车联网应用环境下的数据安全风险，参与各方应当采取一切有效的安全措施确保数据的安全性和保密性，例如对通信通道进行加密、为每辆车设置独立的加密密钥管理系统、验证数据接收设备等。

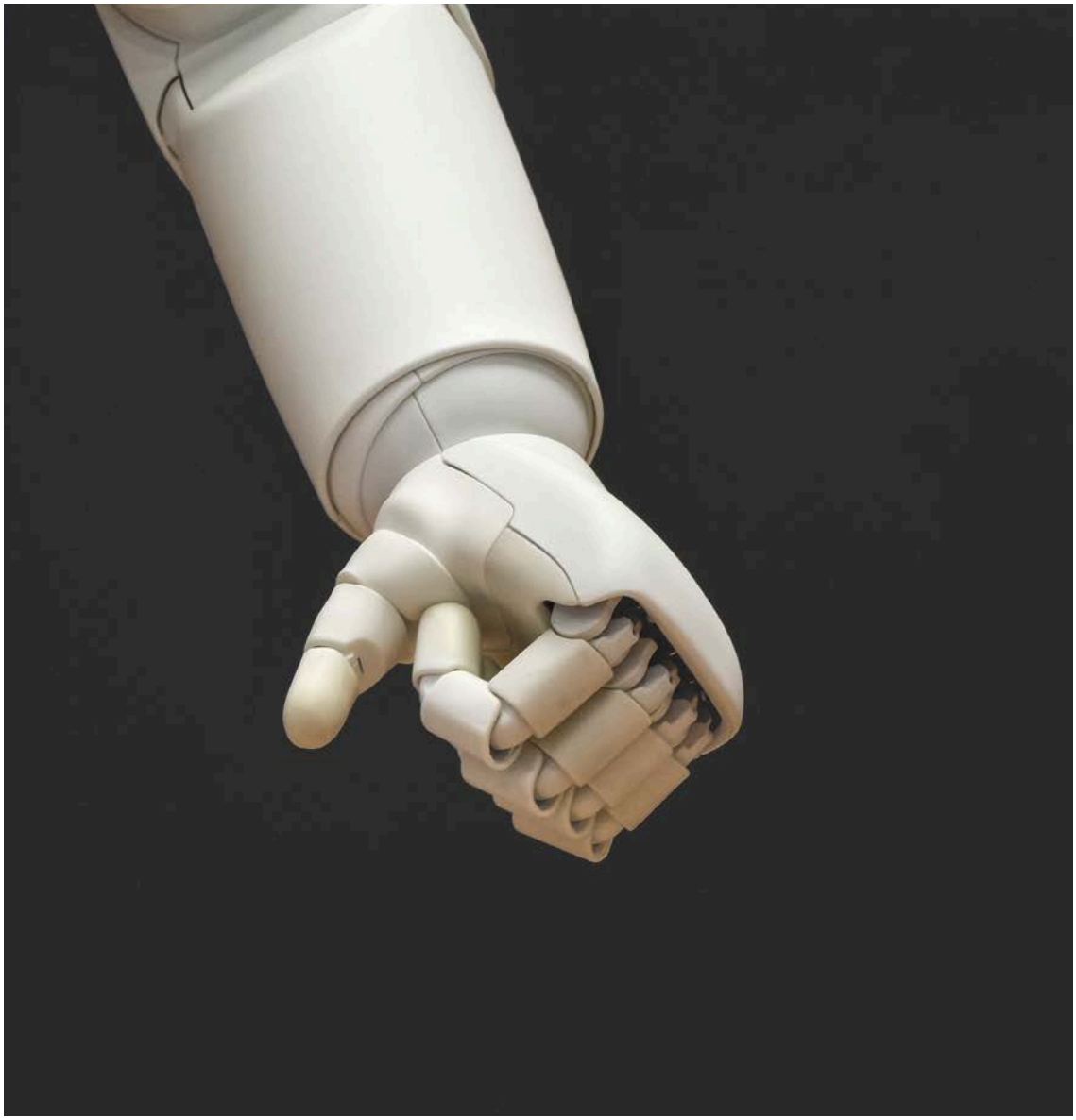
《车联网个人数据保护指南》尤其强调了汽车制造商应采取的安全措施：①区分车辆的重要功能与完全依靠通信能力的功能（例如娱乐功能）；②实施技术措施确保能够在车辆的整个使用周期内能够迅速修复安全漏洞；③设置防止车辆系统遭受网络攻击的预警系统；④存储访问车辆信息系统的日志记录等。

结语

2020年2月，国家发改委等11个部委联合出台了《智能汽车创新发展战略》[10]，加快推进智能汽车创新发展。2021年5月12日，国家互联网信息办公室发布了《汽车数据安全管理若干规定（征求意见稿）》并公开征求意见，是首个汽车行业数据安全方面的管理规定。各地也纷纷出台相关地方政策落实智能网联汽车产业的推动战略，相关法规及技术标准也在陆续制定和完善中。车联网应用环境，特别是人工智能与车联网结合应用的情况下，个人数据保护问题关系着个人的基本权利和自由。无论是车辆制造商还是各类服务提供商，都应充分重视，共同建立车联网应用环境下良好的个人数据保护生态。

为帮助企业更好的理解中国及欧盟复杂的数据保护执法监管环境，更有效的降低法律风险，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，对国内外立法及政策走向及时进行解读。

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



人工智能技术出口管制问题

作者/蔡荣伟、陈坤

近年来，人工智能技术在新一轮的科技竞争中逐渐占据重要地位，关于人工智能技术的出口规制也已然成为中美经济及科技博弈的新战线。2020年1月和8月，美国和中国先后增加了对人工智能相关技术出口的限制，此外，结合此前部分中国企业旗下的APP在美国被禁止运营的一系列风波，以及最近监管机构对企业境外上市采取的网络安全审查措施，都突显了主权国家对数据和技术出境对国家安全和国家经济影响的重视。本文限于篇幅原因，暂不探讨与人工智能有关的国家安全和网络安全审查问题，仅对我国人工智能技术出口管制问题做详细论述。

PART 01

中国的出口管制制度、技术进出口禁限管理制度及不可靠实体清单制度

国内企业能否出口人工智能技术涉及到国家对于企业的对外贸易管制问题。我国对外贸易方面的管制目前可分为三项制度体系，分别是出口管制制度、技术进出口禁限管理制度以及不可靠实体清单制度。了解前述三个制度，厘清其各自规制的范围及侧重点，是明确人工智能技术出口管制问题的必要前提。

1.三种制度体系及其相关法律法规

（1）出口管制制度

出口管制制度对维护国家安全和利益、履行防扩散等国际义务相关的物项进行出口管制。管制物项包括货物、技术、服务等物项以及与物项相关的技术资料等数据。也就是说，该制度及其相关规定所管制的物项包括有形物体和无形的技术和服务。目前，管制物项可主要划分为十类，分别是：核，核两用品及相关技术，生物两用品及相关设备和技术，化学品及相关设备和技术，导弹及相关物项和技术，易制毒化学品，商用密码，军品，部分两用物项与技术（如无人驾驶航空飞行器或无人驾驶飞艇）和特殊民用物项（如吸沙船）。

（2）技术进出口禁限管理制度

技术进出口禁限管理制度对从中国境外向中国境内，或者从中国境内向中国境外，通过贸易、投资或者经济技术合作的方式转移技术的行为进行管理。也就是说，该制度及其相关法规仅对技术的进出口进行管理。目前，其

管理的技术涉及农、林、牧、渔、计算机服务业、软件业等33个行业的一百多项技术。

（3）不可靠实体清单制度

根据不可靠实体清单制度，国家可对在国际经贸及相关活动中的危害中国主权、安全、发展利益或违反中国正常的市场交易原则等的外国实体采取限制进出口活动等处理措施。外国实体一旦被列入清单，将在贸易、投资、人员及交通工具入境等方面被采取相应的限制或者禁止措施。也就是说，该制度及其相关规定所针对的是外国个人或单位（包括公司和团体）。

关于该三种制度体系的主要相关法律法规下表1：

表1：三种制度体系的主要法律法规

制度	主要相关法律法规
出口管制制度	《中华人民共和国出口管制法》 《中华人民共和国对外贸易法（2016修正）》 《中华人民共和国核两用品及相关技术出口管制条例》 《中华人民共和国导弹及相关物项和技术出口管制条例》 《中华人民共和国军品出口管理条例》 《中华人民共和国监控化学品管理条例》 《易制毒化学品管理条例》 《放射性同位素与射线装置安全和防护条例》 《有关化学品及相关设备和技术出口管制办法》 《中华人民共和国生物两用品及相关设备和技术出口管制条例》 《两用物项和技术进出口许可证管理办法》 《两用物项和技术进出口许可证管理目录》 《军品出口管理清单》
技术进出口禁限管理制度	《中华人民共和国对外贸易法（2016修正）》 《中华人民共和国技术进出口管理条例》 《禁止出口限制出口技术管理办法》 《中国禁止出口限制出口技术目录》 《技术进出口合同登记管理办法》
不可靠实体清单制度	《不可靠实体清单规定》

2.三种制度体系的历史与发展

(1) 出口管制制度

从上世纪末至本世纪初，国家先后就“出口管制制度”出台了多项行政法规，对化学品、军品、核两用品、导弹等物项的出口进行管制。此外，2004年《中华人民共和国对外贸易法》（简称“**《对外贸易法》**”）修订，新增的第二十七条[1]在法律层面上赋予了国家对军事有关国际服务贸易和裂变、聚变等物质的国际贸易采取管制措施以维护国家安全的权力，但仍然未改变由多部行政法规对不同领域的物项进行出口管制的现象。立法分散、法律效力位阶等级低、立法时间较为久远等问题给监管执法实践带来诸多弊端。直至2020年10月17日，备受关注的《中华人民共和国出口管制法》（简称“**《出口管制法》**”）经第十三届全国人大常委会第二十二次会议正式表决通过，并于2020年12月1日生效实施。《出口管制法》结束了中国政府在出口管制方面由多部分散的行政法规进行物项出口管制的局面，在法律层面构建了中国出口管制制度的基本框架和程序规则。

(2) 技术进出口禁限管理制度

中国的技术进出口禁限管理制度的立法依据是《对外贸易法》。该法于1994年颁布，根据该法的第十六条，国家可基于“国家安全”等原因禁止或限制某些技术的进出口。但之后的几年，中国政府并未颁布相关实施法规和执法措施，直至2001年的911恐怖袭击事件发生，为履行联合国多边义务，中国政府于2001年底迅速出台了多项出口管制法律法规，包括《中华人民共和国技术进出口管理条例》《禁止出口限制出口技术管理办法》《中国禁止出口限制出口技术目录》。至此，中国关于技术进出口禁限管理制度基本形成。2020年8月28日，国家商务部和科学技术部发布了《关于调整发布<中国禁止出口限制出口技术目录>的公告》，这是时隔12年之久国家再次对《中国禁止出口限制出口技术目录》的调整，而此次调整就涉及对人工智能相关技术的出口限制。

(3) 不可靠实体清单制度

在不断变化的国际形势下，2019年5月31日，中国商务部首次通过新闻发布会宣布，中国将建立“不可靠实体清单制度”。2020年9月19日，经国务院批准，商务部公布《不可靠实体清单规定》，该规定依据《对外贸易法》和《中华人民共和国国家安全法》制定并出台。这是中国首次出台不可靠实体清单制度的相关规定，关于建立“不可靠实体清单制度”的目的，商务部发言人曾表示，是为维护国际经贸规则和多边贸易体制，反对单边主义和贸易保护主义，维护中国国家安全、社会公共利益和企业合法权益[2]。但截止目前，尚

1.《对外贸易法》（2004年修订）第二十七条　国家对与军事有关的国际服务贸易，以及与裂变、聚变物质或者衍生此类物质的物质有关的国际服务贸易，可以采取任何必要的措施，维护国家安全。在战时或者为维护国际和平与安全，国家在国际服务贸易方面可以采取任何必要的措施。

未有外国企业、其他组织或个人被列入该清单。

2.参见商务部网站http://www.mofcom.gov.cn/xwfbh/20190531.shtml

3.三种制度体系对人工智能相关技术出口的影响

根据我们对中国的出口管制制度、技术进出口禁限管理制度及不可靠实体清单制度的介绍可知：

(1)出口管制制度规制重点在于对特殊物项的出口进行管制，这些特殊物项关乎国家安全和利益。但审视目前的《两用物项和技术进出口许可证管理目录》和《军品出口管理清单》所规制的具体物项，暂不包含人工智能相关技术，但不排除将来可能会包含人工智能技术或物品。

(2)不可靠实体清单制度的规制重点在于外国实体，针对“人”，但目前尚未有任何清单。

(3)技术进出口禁限管理制度规制的技术范围非常广泛，涉及33个行业的百余项技术，也包含了本文中我们关注的人工智能有关技术。

目前在出口管制制度和不可靠实体清单制度两个体系下，暂没有具体针对于人工智能技术出口方面的管制，所以在下文中我们主要就技术进出口禁限管理制度对人工智能技术出口的管制进行介绍和分析。但我们仍然提请相关读者注意，国际形势瞬息万变，应当密切关注出口管制制度体系和不可靠实体清单制度可能做出的调整，以便于及时采取必要措施调整对外贸易的进程，降低可能招致的法律风险。

PART 02
技术进出口禁限管理制度对人工智能技术出口的管制

根据《中华人民共和国技术进出口管理条例》第二条，技术进出口指的是，“从中华人民共和国境外向中华人民共和国境内，或者从中华人民共和国境内向中华人民共和国境外，通过贸易、投资或者经济技术合作的方式转移技术的行为。”其中，转移技术的行为包括专利权转让、专利申请权转让、专利实施许可、技术秘密转让、技术服务和其他方式的技术转移。例如，某北京企业与某德国企业在今年3月签署了向中国引进德国先进医疗科技的协议，这一行为就是典型的技术进口行为。再比如，如果一家中国企业想在美国运营以AI技术为支撑的APP，且需要由其中国母公司向该APP提供算法等技术支持的，就会涉及技术出口行为。

1.技术进出口禁限管理制度相关法律法规概览

如前文对中国技术进出口禁限管理制度的介绍，该制度的立法依据之初是1994年颁布的《中华人民共和国对外贸易法》，该制度下主要的法律法规包括《中华人民共和国技术进出口管理条例》《禁止出口限制出口技术管理办法》《中国禁止出口限制出口技术目录》。关于技术进出口管理方面，上述法律或法规规制重点如下表2：

表2：法律或法规关于技术出口管制方面的规制重点

法律法规	发布和修订时间	规制重点
《中华人民共和国对外贸易法》	1994年发布，2004年、2016年修订	第十六条原则性地规定了政府可基于“国家安全”等原因禁止或限制某些技术的进出口
《中华人民共和国技术进出口管理条例》（简称“《进出口管理条例》”）	2001年发布，2011年、2019年、2020年修订	为技术进出口管理提供了指导方针
《禁止出口限制出口技术管理办法》	2001年发布，2009年修订	为技术进出口提供了具体指导细则
《中国禁止出口限制出口技术目录》（简称“《出口目录》”）	2001年发布，2008年、2020年修订	详细罗列了限制出口技术和禁止出口技术的名称和控制要点

2.限制出口的人工智能技术

根据《进出口管理条例》，技术的出口分为自由出口技术、限制出口技术和禁止出口技术，《出口目录》中与人工智能相关的技术，主要是被列入限制出口技术。

《出口目录》于2001年首次发布，在2008年和2020年各修订了一次。实际上，2001年和2008年的《出口目录》就限制了多个与人工智能相关技术的出口，如：智能汉字语音开发工具技术，汉字、语音识别技术，汉语或少数民族语音合成技术（2008年），具有交互和自学习功能的脱机手写汉字识别系统及方法。

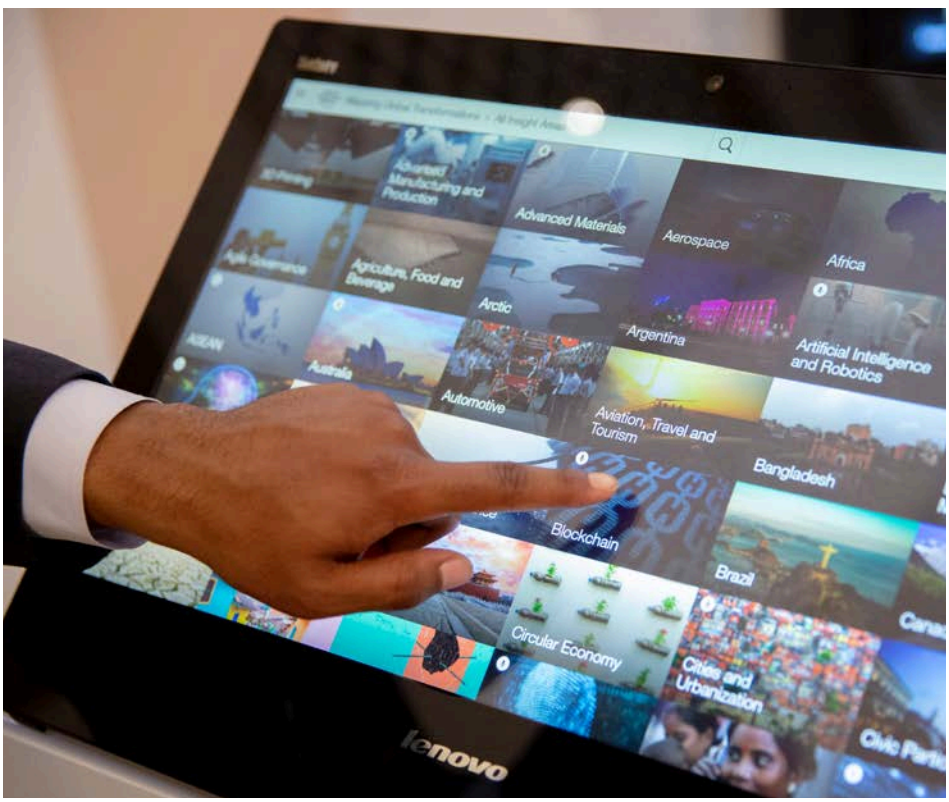
2020年8月28日，国家商务部和科学技术部发布《关于调整发布<中国禁止出口限制出口技术目录>的公告》对2008年的《出口目录》进行修订，其

中在计算机服务业的信息处理技术（编号056101X）项下增加了5项控制要点，包括：语音合成技术，人工智能交互界面技术，语音评测技术，智能阅卷技术以及基于数据分析的个性化信息推送服务技术。此外，在计算机服务业项下的密码安全技术、高性能检测技术、信息防御技术和信息对抗技术中新增的控制要点，以及在软件业项下对基础软件安全增强技术新增的控制要点也可能与人工智能技术有关。

3.对人工智能技术出口的管辖

（1）属地管辖

《进出口管理条例》第二条规定，技术出口行为指的是从中国境内向中国境外，通过贸易、投资或者经济技术合作的方式转移技术的行为。即，不论技术所有权人的国籍或注册地是否为中国，只要相关技术出口行为发生在中国境内就要受到《进出口管理条例》及其相关法律法规的规制。举例来说，美国专利权人将在中国境内产生的人工智能专利技术转移给日本的被许可方，也会受到中国政府的管辖。



(2) 技术转移方式

根据《进出口管理条例》的规定，涉及出口的技术转移行为包括专利权转让、专利申请权转让、专利实施许可、技术秘密转让、技术服务和其他方式的技术转移。

从定义上来看，该规定涵盖的范围十分广泛。从理论上讲，技术转移可以包括以任何形式向其他个人或组织披露和传播技术信息，比如发送电子邮件、提供数据接口或者提供访问权等使得外国的个人或组织可以访问的方式。再比如，如果一家跨国公司的中国子公司作为跨国公司在华设立的外资研发中心，为境外的母公司或关联公司提供研发服务，或与它们联合进行研发，中国子公司则有可能会被认为通过技术服务或其他方式进行技术出口，从而受到《进出口管理条例》的规制。

4.人工智能技术的出口流程

如上文所述，技术的出口分为自由出口技术、限制出口技术和禁止出口技术。自由出口技术指的是不在《出口目录》禁止出口和限制出口范围的技术；限制出口技术指的是《出口目录》所列限制出口的技术；禁止出口技术是《出口目录》所列禁止出口的技术。与人工智能相关的技术，基本上均归为限制出口技术。

我们对《进出口管理条例》及其相关规定关于自由出口技术、限制出口技术和禁止出口技术的出口流程归纳见下表3：

表3：人工智能技术出口流程

规制分类	相关人工智能技术	技术出口流程
自由出口技术	不在《出口目录》之列的人工智能相关技术。例如，计算机视觉的人脸识别技术目前未被列入《出口目录》的禁止出口或限制出口技术范围，应属于自由出口技术	自由出口技术的出口应当办理合同登记，由相关部门形式审查通过后颁发技术出口合同登记证
限制出口技术	根据上文关于“限制出口的人工智能技术”的介绍，《出口目录》限制出口的人工智能相关技术主要包括： ◆智能汉字语音开发工具技术； ◆汉字、语音识别技术； ◆汉语或少数民族语音合成技术；	限制出口技术的出口应当获得出口许可，具体流程如下： ◆向省级商务主管部门进行技术出口申请：在与外方就技术出口交易进行实质性谈判前，技术出口经营者必须向省级商务主管部门提出申请，省级商务主管部门会同省级科

表3：人工智能技术出口流程

规制分类	相关人工智能技术	技术出口流程
	◆具有交互和自学习功能的脱机手写汉字识别系统及方法； ◆语音合成技术（包括语料库设计、录制和标注技术，语音信号特征分析和提取技术，文本特征分析和预测技术，语音特征概率统计模型构建技术等） ◆人工智能交互界面技术（包括语音识别技术，麦克风阵列技术，语音唤醒技术，交互理解技术等） ◆语音评测技术（包括朗读自动评分技术，口语表达自动评分技术，发音检错技术等） ◆智能阅卷技术（包括印刷体扫描识别技术，手写体扫描识别技术，印刷体拍照识别技术，手写体拍照识别技术，中英文作文批改技术等） ◆基于数据分析的个性化信息推送服务技术	技行政主管部门分别对技术出口项目进行贸易审查和技术审查，并在收齐申请材料之日起30个工作日内做出是否批准申请的决定。省级科技行政主管部门在进行技术审查的过程中，可以组织专家对申请出口的技术进行审查 ◆获得有效期为三年的技术出口许可意向书：若技术出口获得批准，省级商务主管部门将颁发由商务部统一印制和编号的《中华人民共和国技术出口许可意向书》（简称“《许可意向书》”）给技术出口经营者，《许可意向书》的有效期为三年。技术出口经营者可以凭《许可意向书》与外方进行实质性谈判，签订技术出口合同。在未取得《许可意向书》前，任何单位和个人都不得对外进行实质性谈判，不得做出有关技术出口的具有法律效力的承诺 ◆获得技术出口许可：在技术出口合同签署以后，技术出口经营者应将签订的技术出口合同副本，连同《许可意向书》以及其他申请文件提交给省级商务主管部门。省级商务主管部门在收齐前述文件15个工作日内，对技术出口作出是否许可的决定。若省级商务主管部门对技术出口作出许可决定，则会向技术出口经营者颁发《技术出口许可证》。技术出口合同自《技术出口许可证》颁发之日起生效
禁止出口技术	目前《出口目录》所列禁止出口技术暂不包含人工智能相关技术。但需要注意，在进行人工智能技术出口时，如相关技术被认定为禁止出口技术，例如人工智能技术涉及到我国政府、政治、经济、金融部门使用的涉及国家秘密的信息安全保密技术的，则会被禁止出口	不得以任何方式出口禁止出口技术

5.法律责任

《进出口管理条例》第四十四条明确规定了非法出口禁止或者限制技术的法律责任，包括行政责任和刑事责任。如果情节尚不构成刑事责任的，违法进行技术出口的相关主体可能会被给予警告，没收违法所得，处违法所得1倍以上5倍以下的罚款，直至撤销其对外贸易经营许可等。如情节严重的，应依照《中华人民共和国刑法》关于走私罪、非法经营罪、泄露国家秘密罪或者其他罪的规定，依法追究违法技术出口经营者的刑事责任。

此外，若技术出口经营者受到行政处罚或刑事处罚，那么自行政处罚决定生效之日或者刑事处罚判决生效之日起，国务院有关部门可以在三年内不受理该经营者提出的进出口配额或者许可证的申请，或者禁止该经营者在一年以上三年以下的期限内从事有关技术的进出口经营活动。

6.影响及建议

国家商务部和科技部在调整发布《出口目录》的答记者问中提到，接下来将进一步删减《出口目录》，优化技术贸易营商环境、积极推进技术贸易便利化[3]。在此大背景下，《出口目录》却加强了对人工智能相关技术的出口限制，突显了国家对相关人工智能技术出口带来的各方面影响的高度关注，相关规制措施也定会直接或间接地影响到人工智能技术的跨国贸易、投资及合作活动。如前所述，如果一个中国AI科技公司在境外设立子公司，并向该子公司提供AI技术，严格意义上讲，应按照《进出口管理条例》的规定履行申请许可程序。而如果该子公司与境外公司合资经营，或被并购，则更需要履行申请许可程序。

鉴于国家对于人工智能技术出口的关注以及《进出口管理条例》所规定的严格法律责任，我们建议相关企业应对人工智能技术的出口予以高度重视，并采取如下措施：

（1）加强对可能涉及《出口目录》技术项目的内部审查和审批流程，包括：

1)应当对企业所涉及的贸易、投资和合作行为或计划是否涉及《进出口管理条例》所规定的技术出口行为进行审查。技术出口行为包括从境内向境外通过专利权转让、专利申请权转让、专利实施许可、技术秘密转让、技术服务和其他方式进行技术转移的行为。在此建议读者，应当注意审查容易被忽视的技术出口行为，例如通过电子邮件、提供数据接口或者提供访问权的方式向境外提供技术，或作为跨国企业的在华子公司与境外的母公司或关联企业开展研发合作，即使约定专利权和专利申请权及其他知识产权均由境

3.参见商务部网站 http://www.mofcom.gov.cn/article/ae/sjjd/202008/20200802996696.shtml

外公司所有，根据属地原则仍会被视为技术出口，受技术出口法律规制。另，在受限的人工智能项目中如有外籍人士参与，也会有类似风险。

2)对于涉及技术出口行为的，应初步评估相应技术是否可能属于《出口目录》所限制出口的人工智能相关技术：

a)对于不属于《出口目录》所限制的人工智能技术的出口，应当办理技术出口合同登记。

b)对于属于受到出口限制的人工智能技术的，应在获得监管部门许可意向后，再进行技术出口的实质性谈判，并在获得技术出口许可证后再签署技术出口相关合同。

(2)密切关注人工智能技术进出口禁限管理方面的最新立法动态，包括是否增加限制出口的人工智能技术、人工智能相关技术是否会被列入禁止出口技术、人工智能相关技术是否会被列入出口管制的物项，以及，实时关注不可靠实体清单的更新情况。

(3)密切关注监管部门对于人工智能技术出口方面的执法动态。虽然到目前为止，鲜有公开报道提及公司因技术出口行为未取得技术出口许可而受到处罚，但在《出口目录》新修的背景下，人工智能技术的出口很可能会受到监管部门的特别关注，相关执法动态可作为判断企业出口法律风险的风向标。

在今年7月8日举办的2021世界人工智能大会治理论坛上，由中国科学技术信息研究所研究发布的《2020全球人工智能创新指数报告》显示，中国人工智能创新指数在参评国家中排名第2位，仅次于美国，是排名前十的国家中唯一的发展中国家[4]。

人工智能技术是我国经济发展中的一次重要机遇，或可成为引领我国新一轮产业变革的核心与关键驱动力，将推动数万亿数字经济产业转型升级。在世界局势波诡云谲的当下，人工智能技术出口管制成为大国之间博弈的一个特写，各国也必将根据不断变化的国际形势调整相关管制措施。建议人工智能行业的企业和个人实时关注境内外关于人工智能技术的政府管制动态，并适时采取措施防范风险。

4.参见https://baijiahao.baidu.com/s?id=1704700056994520998&wfr=spider&for=pc

蔡荣伟
合伙人
公司业务部
上海办公室
+86 21 6061 3175
roncai@zhonglun.com

中倫律師事務所
ZHONG LUN LAW FIRM

中伦研究院出品