

DOI: 10.13766/j.bhsk.1008-2204.2024.0751

**编者按:**近期,《人工智能法(学者建议稿)》《人工智能示范法2.0(专家建议稿)》等人工智能立法建议稿相继涌现,加速推动人工智能立法成为学界主流观点。然而,人工智能立法的立法目标、立法体系、具体规则等事项依然存在较大争议。为此,本刊特刊发专题笔谈,邀请了来自北京航空航天大学、中国政法大学、西北政法大学、中国信息通信研究院、中国社会科学院、华东政法大学、西南政法大学等多所院校的知名专家,就人工智能立法的立法逻辑、立法体系、内容模块等核心议题进行了深入的理论探讨和观点交流。

## 人工智能法:必要性与可行性

杨建军<sup>1</sup>, 张凌寒<sup>2</sup>, 周辉<sup>3</sup>, 程莹<sup>4</sup>, 郑志峰<sup>5</sup>, 韩旭至<sup>6</sup>,  
赵精武<sup>7</sup>, 周瑞珏<sup>7</sup>

(1. 西北政法大学, 陕西 西安 710063; 2. 中国政法大学, 北京 100088; 3. 中国社会科学院, 北京 100009;

4. 中国信息通信研究院, 北京 100083; 5. 西南政法大学, 重庆 401120; 6. 华东政法大学, 上海 201620;

7. 北京航空航天大学, 北京 100083)

中图分类号: D922.17; TP18

文献标志码: C

文章编号: 1008-2204(2024)03-0162-13

### 人工智能法的核心立法目标: 安全与发展并重

#### 一、人工智能的安全与发展 是辩证统一的

人工智能是否安全,如何保障其安全发展,是全球关注的焦点问题。人工智能既具有技术属性,也具有社会属性。人工智能安全发展的目标,在于更好地造福人类社会。联合国教科文组织、欧盟、美国、日本等的人工智能立法和相关文件高度关注人工智能的安全发展问题。

中国也高度关注人工智能发展的安全问题。人工智能技术的科学发展,有助于更好地保障国家安全。国务院印发的《新一代人工智能发展规划》指出,“人工智能是引领未来的战略性技术,世界主要发达国家把发展人工智能作为提升国家竞争力、维护国家安全的重大战略”,要求“建设安全便捷的智能社会”“利用人工智能提升公共安全保障能力”“构建泛在安全高效的智能化基础设施体系”。

人工智能技术,可以广泛应用于公共安全和自

然灾害的智能化监测预警、社会治理、新型犯罪侦查、反恐等多个领域。因而,人工智能技术的发展,有助于提高国家的总体安全能力。

安全是人工智能长远发展的前提和基础,因此,人工智能立法应当将维护国家安全作为立法的目的之一,将安全作为一种价值观贯穿立法始终,将“安全可问责”作为一项基本原则明确写入文本,并通过更加具体、科学的制度设计,有效管控人工智能的安全风险。

#### 二、人工智能立法如何保障安全

人工智能安全包括哪些基本含义?《人工智能安全标准化白皮书(2023版)》指出,人工智能的安全性包括网络安全属性和系列安全属性。网络安全属性,即“人工智能系统及其相关数据的机密性、完整性、可用性以及系统对恶意攻击的抵御能力”。系列安全属性,即:一是人工智能的可靠性,即在不利或有害环境下“仍能按照既定的目标运行、保持结果有效”;二是透明性;三是可解释性;四是公平性,即人工智能模型决策结果客观、中立,无歧视;五是隐私性。人工智能的安全问题,通常表现为利用用户数据进行训练容易导致隐私信

息泄露、算法的可解释性目标难以达成、人工智能技术被滥用。人工智能安全至少应当包括技术安全、稳健、无害、非恶意、预防、保护、完整性等<sup>[1]</sup>。当然,需要指出的是,由于世界各国和地区对“安全”概念的理解存在差异,因而不同语境下“安全”概念的外延也可能有一定的不同。

尽管如此,人工智能立法还应同时注重维护国家安全、人工智能技术发展和创新安全、个人信息和隐私安全,涵盖人工智能的内生安全、衍生安全和发展安全。中国的人工智能立法,至少应从以下方面,建立人工智能安全监管的相关制度体系。

其一,安全应成为人工智能立法的基本立法目的之一。人工智能安全,事关国家的总体安全,人工智能的安全风险会波及国家、社会、企业和个人。因而,人工智能的发展,应首先注重防止针对人工智能的攻击、干扰、破坏、非法使用和意外事故,在确保自身安全的前提下,保障、促进人工智能技术、产业和应用的发展。为此,应将安全作为人工智能立法的立法目的和基本原则写入文本,并将人工智能安全理念贯穿人工智能立法始终,融入人工智能立法的灵魂。

其二,人工智能立法,应同时注重维护国家安全、人工智能技术发展和创新安全、个人信息和隐私安全。一是国家应支持相关主体开展网络等基础设施的安全、数据安全和算法安全技术的开发应用,加快安全技术创新,支持相关专业机构依法提供服务,防止技术偏见、算法歧视和数据泄露,更好地保护数字隐私,防止社会伦理风险。二是明确人工智能开发者、提供者负有的安全保障、安全风险评估、重大安全事件报告、维护网络信息内容安全、维护保险标的安全等法律义务。三是应对关键人工智能的开发提出更高的法律要求,明确关键人工智能开发者、提供者将安全措施建设与关键人工智能同步规划、同步建设、同步使用的义务,具体可通过包括关键人工智能的风险评估、安全风险披露、应急处置等义务来促进安全义务的落实。四是将安全作为重要价值,植入行政人工智能、司法人工智能、新闻人工智能、医疗人工智能、社交机器人、生物识别、自动驾驶汽车、社会信用人工智能、通用人工智能管理等特殊应用场景中的人工智能开发和应用的相关条款。五是注重推进人工智能治理的国际合作,因为人工智能的风险,无法依靠单一国家予以有效应对。此外,应将在中国境外

开展人工智能开发、提供、使用活动,并可能影响中国国家安全、公共利益或者个人及组织合法权益的行为纳入本法管辖范围,更好地维护国家主权。

其三,立法应当防止人工智能不当应用引发的社会治理风险。为此,应特别注重基于执法目的对于人工智能技术使用的合理规制。例如,应当禁止使用个人的面部或指纹等基于自然人的生物数据对个人进行的特定评价,防止针对自然人提供社会评价的人工智能系统技术的使用,防止对自然人在工作、生活教育场景中的情绪状态检测技术的使用,防止深度伪造技术的使用,防止因技术的不当使用而造成对个人的社会歧视或者不公平对待。此外,人工智能安全法律制度的设定,还应注意与关联法律制度的衔接,因为人工智能技术的发展,会引发人格权保护、知识产权保护、数据财产保护、侵权责任认定等关联法律问题<sup>[2]</sup>。

还需特别指出的是,在人工智能立法过程中,应特别注重与《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《互联网信息服务算法推荐管理规定》等关联法律法规和规范性文件在总体上保持协调和一致,更好地维护立法的科学性。人工智能立法既应立足中国国情,也应积极借鉴和吸纳全球人工智能立法的先进经验。“总体来看,多数西方国家对人工智能的应用比较慎重,呈现出一种‘保守倾向’。”<sup>[3]</sup>例如:在英国,即便是执法机构使用人脸识别技术,也应当受到英国《保护自由法》《平等法》《人权法》等法律的约束;在法国,《法国数据保护法》规定,“未经同意,无论是公营还是私营的运营者,都必须经过法律授权才能处理生物特征识别数据”,以更好地保护公民的“匿名权”;在美国,一些知名企业,如IBM,于2020年宣称“不再提供通用的人脸识别或分析软件”,并坚决反对“将技术用于大规模建设、种族歧视、侵犯基本人权和自由”<sup>[4]</sup>。此外,欧盟对人脸识别持谨慎态度,瑞典、比利时等国家也对人脸识别技术做了一定的限制<sup>[5]</sup>。欧盟《人工智能法》对公共场所人脸识别技术、生物识别技术使用的严格管控等,都是未来中国立法中应当高度关注的重要立法动向。

总之,人工智能立法,应坚持以人为本、促进智能向善,兼顾安全、发展与治理,平衡好创新与监管之间的关系,在管控好技术安全和社会风险的前提下,更好地促进人工智能技术和产业的发展,

增进人类福祉,防止因过于严苛的管控而遏制人工智能技术发展的生命力和创造力。

——杨建军(西北政法大学法治学院、数字法学研究院教授)

#### 参考文献:

- [1] 周辉,徐玖玖,朱悦,等.人工智能治理:场景、原则与规则[M].北京:中国社会科学出版社,2021:33.
- [2] 王利明.人工智能时代提出的法律问题[M]//任仲文.人工智能领导干部读本.北京:人民日报出版社,2017:181—184.
- [3] 姜伟.法律人工智能导论[M].北京:北京大学出版社,2023:20.
- [4] 梁正,薛澜,张辉,等.人工智能治理框架与实施路径[M].北京:中国科学技术出版社,2023:92—93.
- [5] 王森,杨捷.人脸识别发展与监管研究[M]//赵岩.人工智能发展报告(2020—2021).北京:电子工业出版社,2021:175—176.

## 《人工智能法(学者建议稿)》: 如何以“善治”促“善智”

当今时代,人工智能作为引领未来变革的战略技术,在重塑生产方式、优化产业结构、提升生产效率、赋能千行百业的同时,也带来了安全、隐私、公平等方面的一系列问题和挑战。面对人工智能的迅猛发展和与之相伴的复杂风险,中国于2023年10月发布了《全球人工智能治理倡议》,呼吁坚持“以人为本”理念和“智能向善”宗旨,促进人工智能技术造福人类。2024年年初,李强在出席世界经济论坛2024年年会时再次强调,要“以‘善治’促‘善智’,引导人工智能朝着有利于人类文明进步的方向发展”<sup>[1]</sup>。

人工智能产业的健康发展,离不开包容审慎、行之有效的良法善治。放眼国际,新一代人工智能技术的可持续发展竞争,不仅是技术层面的竞争,也是法治软实力的竞争。2024年3月21日,联合国大会未经表决一致通过了全球首个关于监管人工智能的决议——《抓住安全、可靠和值得信赖的人工智能系统带来的机遇,促进可持续发展》,这一决议具有里程碑意义。世界主要人工智能使用国的立法工作也皆在紧锣密鼓的推进当中。美国作为全球人工智能产业的领跑者,于2023年10月由拜登签署了《关于安全、可靠和可信地开发和使

用人工智能的行政令》。而欧盟经过内部长达3年的筹备与谈判,于2024年3月正式通过《人工智能法》,这是全球首部关于人工智能系统的立法。

## 一、“以人为本”引导人工智能 “向善”发展

人工智能发展对“人”的影响一直备受关注,坚持“以人为本”治理理念是实现人工智能“向善”发展的基本要求。《人工智能法(学者建议稿)》在制度设计上积极贯彻《全球人工智能治理倡议》中“以人为本”的人工智能治理主张,与联合国“为人类治理人工智能”(Governing AI for Humanity)的行动宗旨保持一致,高度重视伦理、使用者权益与数据安全。

首先,人工智能立法应当坚持法治与德治相结合,将科技伦理审查原则置于所有基本原则首位,强调人工智能产业发展过程中科技伦理的重要调控作用,确保人工智能发展符合人类社会价值。

其次,人工智能立法应当坚持任何技术的创新发展都不应以牺牲个人权益为代价,人工智能的技术应用必须充分尊重个人权益。《人工智能法(学者建议稿)》设置了“个人权益保障”专章,明确保护人工智能使用者的平等权、知情权、隐私权、拒绝权等权利。同时,《人工智能法(学者建议稿)》还特别关注数字弱势群体可能面临的数字鸿沟问题,明确人工智能开发者、提供者应当专门增设面向数字弱势群体权益保护的特殊功能模块。

再次,人工智能立法应当关注从社会整体层面为公众利益提供保障。在教育领域,人工智能立法提出,推进人工智能相关学科建设,开展人工智能相关教育和培训,采取多种方式培养人工智能专业人才。为了提升全民数字素养,人工智能立法支持实施全民数字素养与技能提升行动,以提升公民的数字获取、制作、使用、评价、交互、分享、创新、安全保障、伦理道德等素质和能力。

最后,人工智能立法应当筹划政府主导、社会协同、公众参与的人工智能治理机制,构建多元共治的人工智能治理格局。

上述机制安排能够有效提升公众在人工智能治理中的参与度、知情权和监督能力,更加充分地保障公众权益。



## 二、以“促发展”推动人工智能实现“善智”

“善智”的实现需要发展,而设计良好的“善治”能够有效促进发展。在目前全球激烈竞争的格局中,“不发展是最大的不安全”<sup>[2]</sup>。人工智能立法应当立足中国“领先的追赶者”的国际生态地位,理应设置“促进与发展”专章,在监督管理、责任设置等方面减轻人工智能产品和服务提供者的义务,以实现产业创新予以一定的容错空间和责任豁免的立法目标。

首先,人工智能立法中的“促进与发展”专章可以从国内人工智能企业的发展需求切入,围绕算法、算力、数据人工智能发展三要素设置促进措施。在算力层面,加强算力基础设施建设,建立算力基础设施资源调度机制,推动公共算力资源平台的建设与利用;在算法层面,支持关键技术创新,加强算法模型保护,推进开源生态建设;在数据层面,提升高质量数据要素供给能力,建立人工智能产业数据资源统筹机制,建立人工智能数据资源共享机制。

其次,人工智能立法应当审慎界定和划分监管对象和监管手段,在确保安全的同时释放人工智能创新发展空间。人工智能立法对于科学研究活动和免费开源的人工智能应当给予除外豁免,同时增设关键人工智能监管制度。关键人工智能是指应用于关键信息基础设施的人工智能,对个人的生命、自由、人格尊严等人身权益有重大影响的人工智能,以及达到一定能力级别的基础模型等人工智能产品和应用。关键人工智能开发者和提供者需要在组织机构、风险评估、风险披露、安全应急处理等方面承担更多的义务。这一制度能够充分减轻一般人工智能开发者和提供者的负担,在确保安全的基础上激发产业活力,促进人工智能产业的发展。

最后,人工智能立法应当充分考虑企业的合规负担并设置免责事由。一方面,明确利用基础模型以及开源基础模型从事人工智能研发、提供、使用活动的,由衍生利用一方承担法律责任,同时,基础模型提供者需要承担适当的注意义务;另一方面,需要增设合规免责条款,明确开发者、提供者、使用者在合规基础上可以相应豁免行政和刑事责任。

## 三、“治当下,谋长远”持续追求“善智”目标

人工智能产业的突出特点是发展的不确定性,“善治”必须“治当下,谋长远”,如此才能持续推动人工智能向善发展。为了应对人工智能发展的不确定性,人工智能立法应当采用可迭代的人工智能监管体系。

一方面,人工智能立法应当创设动态的人工智能分级分类监管机制。在分级分类监管时,由人工智能主管部门根据人工智能在经济社会发展中的重要程度,以及对国家安全、公共利益或者个人及组织的合法权益可能造成危害的程度,进行分级分类监督管理,依法对关键人工智能实施特殊监管。随着人工智能技术的不断发展,主管部门根据技术发展、行业领域、应用场景等因素进行评估并动态调整分级分类标准,及时更新人工智能分级分类指南。动态分级分类制度可以有效避免“一刀切”式的不合理监管,并且能够持续适应技术发展进步,实现敏捷治理。

另一方面,人工智能立法应当构建人工智能风险防控和应急响应机制,以及时应对人工智能发展中不可预见的风险。人工智能主管部门制定人工智能安全监测预警和信息通报制度,加强人工智能安全信息收集、分析和通报工作,按照规定通报人工智能安全监测预警信息。人工智能主管部门建立健全人工智能应急工作机制,按照危害程度、影响范围等因素对人工智能安全事件进行分级,制定相应的应急预案并定期组织演练。

目前,全球正在经历新一轮人工智能监管浪潮,人工智能国际治理需要更多的中国参与。因此,人工智能立法应当以更加体系化的立法逻辑建构具体内容架构和具体规则。核心的立法目标应当定位于,推动建立健全中国人工智能治理体系,确保技术发展与社会价值观的和谐统一,引导和规范中国人工智能产业健康、有序、“向善”发展。

——张凌寒(中国政法大学数据法治研究院教授)

### 参考文献:

[1] 陈尚文,颜欢,禹丽敏.李强出席世界经济论坛2024年年会并发

表特别致辞[N]. 人民日报, 2024-01-17(1).

[2] 王迪, 张慧中. 李强同德国工商界代表座谈交流[N]. 人民日报, 2023-06-20(2).

## 《人工智能示范法 2.0 (专家建议稿)》—— 人工智能法的立法架构: 原则、体例与创新

新一代人工智能将推动新质生产力的快速发展,带来新一轮科技革命。但是,人工智能技术在优化服务质量、满足生活需求和提高生产效率的同时,也可能带来网络安全、数据安全、个人信息保护等方面的新风险,对现有的人工智能伦理及监管秩序构成新挑战。为了更好地发挥人工智能推动科技跨越发展、产业优化升级、生产力整体跃升的驱动作用,需要积极主动推进人工智能相关立法工作,既采取措施有效防控相关风险,也为人工智能发展提供制度和资源供给等方面的必要支持。

### 一、人工智能立法活动的基本原则

2023年8月,在立足中国人工智能治理经验、把握人工智能发展规律和全球治理趋势的基础上,《人工智能示范法 1.0(专家建议稿)》公开发布。随着社会各界反复研讨交流与人工智能治理不断取得新进展,目前已迭代至《人工智能示范法 2.0(专家建议稿)》。

第一,人工智能立法应当顺应人工智能发展的需要。人工智能立法要平衡好人工智能发展与安全之间的关系,以高质量发展促进高水平安全,以高水平安全保障高质量发展。为此,一方面,人工智能立法需要着眼于破除发展过程中的束缚、障碍,规定技术创新应用的容错机制;另一方面,人工智能立法应当注重建立能够满足发展需要的监管框架,提升监管可预期性,创新监管方式,设计科学的责任义务。此外,人工智能立法还应当充分考虑人工智能技术应用更新迭代较快的特点,增强立法内容前瞻性,既要在充分研究论证的基础上进行必要的制度设计,也要对目前不便于形成结论的问题,采取在指明原则方向基础上留出未来完善与衔接空间的做法。

第二,人工智能立法应当能够有效防范风险。目前,中国已在人工智能治理方面进行了一些立法探索,陆续出台了《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》《科技伦理审查办法(试行)》等规则,并有《深圳经济特区人工智能产业促进条例》等地方性立法实践。但由于已有立法位阶不高,在调整范围、规制手段上仍然有限。为厘清人工智能技术研发、提供和使用的法律边界,人工智能立法需要在明确一般性人工智能安全风险治理措施的同时,对高风险人工智能、基础模型研发等问题进行专门的制度设计。

### 二、人工智能立法的体系框架

结合学界现有研究成果以及人工智能技术治理实践经验,在篇章结构上,人工智能立法更适宜采用“基本原则、促进发展举措、风险管理制度、主体责任分配、治理机制设计、法律责任”这一体系框架。各部分主要内容分述如下。

第一章“总则”,应当阐明人工智能发展与治理应遵循的基本原则,包括治理原则、人类自主原则、安全原则、透明可解释原则、公平原则等。在“总则”确立的原则基础上,下述各章将围绕“总则”展开,并与相关条文呼应。

第二章“人工智能发展”,应当明确国家采取有力措施鼓励人工智能创新。本章可结合产业发展实际,从基础设施、人才培养、技术创新、体制机制支持等维度提出相应制度规范,如对基础模型研发过程中的个人信息保护义务作出减免、促进人工智能开源生态建设等。本章还应强调,以国家机关的先行先试促进人工智能的推广应用,并在保证国家法治统一的前提下提出建立人工智能特区,赋予特区所在市以更大的人工智能治理自主权。

第三章“人工智能管理制度”,应当明确负面清单管理制度,进而对人工智能进行风险管理。对于风险分类分级管理方式,人工智能立法起草专家组认为,鉴于人工智能技术迭代迅速、未来发展潜力较大,应避免风险分类分级标准不明,影响企业的经营预期、提高其合规成本。因此,本章具体内容可包括:负面清单内的研发、提供活动采取许可机制,实行事前监管;负面清单外且达到一定用户规模的提供活动则采取备案机制,实行事后监管;

仅进行人工智能研发活动,或用户数未达标准的提供活动,则无须履行备案义务。这一设计旨在减轻人工智能研发、提供等活动的审查、许可等环节的成本,既能有效防范关键风险,又能容许创新发展。

第四章“人工智能研发者、提供者义务”,应当明确人工智能研发者、提供者应承担的相应合规义务。不同主体应承担的一般义务主要包括保障人工智能公平性和可解释性、进行科技伦理审查和安全审查等,并且应将安全义务贯穿人工智能活动整个生命周期,将人工智能治理的基本原则转化为企业可落地、监管可监督的措施及程序。同时,基于人工智能产业链中主体的复杂性,本章第二节和第三节可对人工智能研发者、提供者予以区分,依据其不同活动特点分配主体义务。此外,结合《人工智能法示范法 2.0(专家建议稿)》前述条款设定的负面清单管理制度,本章可针对负面清单内的人工智能研发、提供活动进一步规定相应的义务类型,保障义务与风险一致,坚守安全底线。

第五章“综合治理机制”,衔接“总则”规定,应当明确国家人工智能主管机关职责。例如:依法报告人工智能发展和治理情况,制定人工智能监管规则、指引,组织制定人工智能伦理、安全、管理等方面的标准,组织人工智能技术监测、评估、审计工作。本章还可对人工智能伦理专家委员会的组建、创新监管、协同监管等机制进行规定。

第六章“法律责任”,根据人工智能的风险活动,应当明确不同法律主体相应的法律责任。同时,本章还需要兼顾发展导向,明确尽职免责等制度,允许以免费且开源的方式提供人工智能的主体可在一定条件下减免责任,以为人工智能开源等创新活动的开展提供更加宽松的政策环境。

### 三、人工智能立法的创新要素

基于人工智能相关法律法规,相应的人工智能立法需要在承接既有规则的同时,创新适应于产业实践动态的新兴规则。如此一来,人工智能立法既完成了对已有制度设计的补充和完善,也能够使一部分人工智能治理的新思路新做法以成文法的形式予以确认。具体而言,人工智能立法的创新要素应当包括以下六点。

第一,人工智能立法应当坚持明确人工智能主

管机关,并更加系统地规定其治理职责。在以更高维度对待人工智能治理问题,避免产生重复监管、多头监管“九龙治水”困境的思路的基础上,《人工智能示范法 2.0(专家建议稿)》确定了人工智能主管机关应承担的各项职责,并明确由人工智能主管机关成立人工智能伦理专家委员会,更好地开展人工智能伦理问题研究、指导伦理审查等工作。

第二,人工智能立法应当创新法律主体架构。依据所从事活动类型不同,可将人工智能法律主体区分为研发者、提供者和使用者的三类主体。并在针对这三类主体进行制度设计的基础上,针对国家机关、平台经营者等人工智能提供和使用特殊主体增设专门义务。

第三,人工智能立法应当创新科技创新激励机制。《人工智能示范法 2.0(专家建议稿)》明确提出了完善算力基础设施建设、建设人工智能领域基础数据库和专题数据库、鼓励国家机关先行先试、提供财政和采购支持等有利于人工智能创新发展举措,并在明确人工智能安全风险治理措施的基础上,提出以税收抵免优惠等措施鼓励人工智能研发者和提供者在人工智能安全保障方面进行投入。

第四,人工智能立法应当创新增设许可管理负面清单。将基于负面清单实施的人工智能许可管理制度与负面清单外人工智能活动的备案制度加以明确区分,避免过重的合规负担影响人工智能产业的经营预期。

第五,人工智能立法应当创新促进人工智能开源发展的相关规则。除鼓励运营开源开发平台、开源社区和开源项目,鼓励设立开源人工智能基金会等措施外,人工智能立法还可以创新性地制定专门合规指引、明确责任减免规则等支持人工智能开源生态发展的措施,并鼓励在政府采购中采购符合国家标准的开源人工智能产品和服务。

第六,人工智能立法应当创新构建知识产权创新规则。在研发环节,人工智能立法可以对训练用数据、个人信息的使用作出专门安排,明确建立与人工智能发展相适应的知识产权法定许可和合理使用制度,保障人工智能领域数据要素供给。在提供与使用环节,人工智能立法可以对人工智能生成物的成果保护与侵权认定进行专门规定,保障人工智能创新成果。

人工智能立法应面向前沿技术、面向数字经济、面向未来。人工智能立法的理念、原则和具体

制度设计,不仅需要随着法律和信息技术等领域的理论研究而更新,也需要随着实践发展而不断迭代,以推动在人工智能时代更好地落实总体国家安全观、在法治道路上实现人工智能安全与发展的更好融合。

——周辉(中国社会科学院法学研究所网络与信息法研究室副主任、副研究员)

## 论人工智能法的立法定位

近年来,大模型技术颠覆性、跨越式突破引发通用人工智能新一轮发展热潮,成为各国科技产业竞争的新赛点。人工智能立法是党中央的重大决策部署,对于推动人工智能产业赋能实体经济、促进人工智能应用提升人民生活品质具有重要意义。

### 一、关于人工智能立法定位

当前,人工智能技术尚处于快速发展期,治理体系正在加速构建完善。发挥好一部基础性、全局性法律的重要作用,需要重点关注以下关系。

第一,把握好促进法与管理法的关系。应兼顾好发展和安全的双重目的需求。一方面,应当明确理论研究、人才队伍、数据算力等激励制度,有效回应企业在放开知识产权限制等方面的发展诉求;另一方面,应当遵循底线思维,明确企业义务性规范、国家监管职责等监管要求,采取政企协同发力、过程管控和事后合规宽大处理相结合的敏捷治理思路。

第二,深化行业立法与一般性立法的互动关系。在条文设计上“宜粗不宜细”,可通过原则性规定指导相关行业立法出台,或通过监管沙盒等制度提供实验基础。对于自动驾驶汽车、医疗健康等行业应用领域,有关规范道路测试准入、明确医疗人工智能责任分配规则等条款,建议出台行业立法予以明确。

第三,理顺新法与旧法的关系。《中华人民共和国民法典》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关立法已对深度伪造、人脸识别等作了初步回应。同时,企业普遍反映,人工智能监管落地中难以把握法律和伦理、大模型评估和科技伦理审查之间的关系,存在一定

的交叉重复。人工智能立法应与现有制度设计做好衔接协调,需要明确统一的评估审查制度、相关监管机构等。

第四,处理好国内法与国际治理的关系。当前,全球人工智能发展和治理处于关键窗口期,人工智能法的制定不仅要考虑国内的技术发展、产业需求,还需与国际人工智能治理的趋势和规则保持协调。应具备一定的灵活性、前瞻性和国际视野,为中国参与国际治理提供法律支撑。

## 二、促进发展的人工智能立法制度设计

第一,明确人工智能法的适用范围,划定应当进行重点监管的领域,对其他领域适当放松管制。中国人工智能产业发展正处于领先的追赶阶段,对人工智能不作区分的“一刀切”式监管,不利于激励产业创新,恐进一步拖慢人工智能追赶步伐。欧盟《人工智能法》总体坚持“基于风险”的分级治理框架,风险越小、约束越少,该法大部分义务条款仅适用于高风险人工智能,对通用人工智能则重点监管具有系统性风险的通用目的人工智能。类似地,美国《行政令》的强制披露义务仅针对能力超过GPT-4的超大能力大模型,对当前已上线的大模型基本采取轻监管的态度。中国人工智能立法中应明确监管范围,综合考虑适用场景、技术能力、用户规模等因素,提出高风险人工智能、基础模型等概念并科学划定范围,减轻低风险人工智能企业负担。

第二,增加产业促进条款,为人工智能产业创新提供政策支撑。针对当前中国面临的原创理论缺失、核心供应链产业链韧性不强、受美持续打压等中长期挑战,应在人工智能法中明确相关产业促进政策,弥补中国产业短板弱项。例如:加大财政性资金投入,加强对人工智能基础技术和关键软硬件研发的资金支持;制定产业、金融、政府采购等政策,鼓励、引导社会资本向“补短板”领域聚集,支持设立投资于人工智能的科技捐赠基金;加大税收激励,对重点生态企业、重点项目的运营企业给予税收优惠,提高人工智能相关研发费用的加计扣除比例,针对创投机构对人工智能领域的投资收益探索给予税收减免等优惠;优化人才政策,探索建立适应人工智能发展需要的人才评价机制、项目管



理创新机制、科技成果转化激励机制。

第三,适当放开知识产权作品等数据资源的使用限制。调研发现,国内大模型训练大多使用国外的开源数据集,国内的高质量数据集建设颇为滞后。调研还显示,当前数据集建设推进速度较慢,目前的数据主要来源于地方政府的门户网站、主要新闻网站等,在很大程度上受限于知识产权制度,难以汇聚商业数据、中国知网等高质量数据。目前,国外采取了一些积极开放举措。例如:美国司法判例倾向将使用版权内容进行模型训练纳入“合理使用”范畴;欧盟《人工智能法》规定,参与沙盒测试的企业可以将基于其他合法目的收集的个人信息数据用于人工智能训练,而不需要用户同意;日本政府则直接规定,人工智能训练数据不受版权法限制。中国人工智能法应积极作出知识产权制度的突破性设计,明确满足著作权“合理使用”的条件<sup>①</sup>,放宽企业在知识产权独占性、数据利用合目的性等方面的限制。

第四,优化法律责任制度设计,推动产业创新发展。基于应用商业形态,人工智能产业链逐渐形成:上游包括数据供给方、创作者、底层配合工具等;中游包括文字、图像、音频、视频等数字内容的处理加工方;下游主要包括各类分发平台、消费方、相关服务机构等。供应链条显著拉长,主体类型复杂多变。在出现风险事故或损害侵权时,责任分配失衡成为影响主体创新和产业投资的重要因素。当前立法倾向将责任施加给服务提供者,但从技术实践上来看,服务提供者控制能力弱,将法律责任完全施加给服务提供者不利于人工智能技术的创新发展。从制度优化上来看,建议明确基础模型和衍生利用者之间的责任分配,豁免开源模型的法律风险,建立“通知—删除”避风港规则,明确使用者责任等。

第五,针对中小企业设计部分义务减轻或免除条款,推动中小企业创新发展生态。中小企业普遍在算力数据获取、技术储备、人才招聘方面处于劣势。美国总统拜登签署行政令,要求能源、科研、教育等部门向中小企业提供资金、技术共享、人才引进等支持;欧盟《人工智能法》特地放宽了中小企业进入沙盒的条件、减免中小企业参与测试评估的费用等。调研显示,中国人工智能中小企业普遍对当前的监管制度缺乏认识储备,法律的“一视同仁”可能转化为大型企业的竞争优势,反向遏制中

小企业的创新发展。中国人工智能法应当考虑对中小企业提供相关义务豁免。例如,简化其备案程序、减少登记事项,在进入沙盒条件及评测费用上予以照顾,推动更多企业进入市场,形成各规模企业配套的完整“科技产业圈”。

第六,关注人工智能治理统筹协调问题,为人工智能组织体系预留空间。英国《支持创新的人工智能监管方案》白皮书指出,由于通用大模型涉及领域的广泛性,难以将其纳入任一监管机构的职权范围,应加强中央层面的监管协调。近年来,欧美加紧推进监管组织机构调整,接连成立人工智能新机构。欧盟设立欧洲人工智能办公室,负责监督并确保《人工智能法》的有效实施,并由独立专家组成的科学小组为人工智能监管提供专业支撑。西班牙率先成立欧洲首个人工智能监管机构——西班牙人工智能监管局。美国行政令提出,建立白宫人工智能委员会,负责协调联邦政府各机构的人工智能相关工作。2024年2月,美国众议院两党领袖共同宣布成立人工智能工作组,帮助立法部门提供前瞻性立法建议。人工智能的发展和治理是国家长远战略部署的重要内容,中国人工智能法应考虑未来治理需要,为发展协调机构改革、监管协调机制创新留出探索空间。

——程莹(中国信息通信研究院政策与经济研究所高级工程师)

#### 注释:

- ① 例如,规定使用他人享有在先著作权的作品进行模型训练时,如果该使用行为是对原作品实施的转换性使用,且不得影响该作品的正常使用,也不得不合理地损害著作权人的合法权益,则该使用行为属于著作权合理使用。符合上述合理使用条件的数据使用行为,可以不经著作权人许可,不向其支付报酬,但不应侵权作者的署名权。

## 人工智能法的表白、留白和补白

### 一、人工智能法的表白与留白

当前,人工智能立法已步入新阶段。国外方面,欧盟发布了全球首部《人工智能法》,引领了人



工智能法律治理新风向。国内方面,2023年6月,国务院办公厅印发《国务院2023年度立法工作计划》,明确提出“预备提请全国人大常委会审议人工智能法草案”,一部统一的、综合的人工智能法呼之欲出<sup>[1]</sup>。与此同时,中国学者先后提出了两部人工智能法建议稿:一部是由中国社会科学院牵头起草的《人工智能示范法2.0(专家建议稿)》,一部是中国政法大学等7校共同起草的《人工智能法(学者建议稿)》。这两部建议稿为人工智能立法贡献了学界智慧。

对人工智能法来说,首要目标是对已有人工智能治理经验进行立法层面的表白,以便起到明确规则、提供预期、划定红线的作用。这种表白需要特别关注三个方面:一是当前人工智能伦理治理的经验与共识,人工智能法需要将其提炼、转化为立法,以便为人工智能治理提供原则性指导,确保人工智能监管的从容性、伦理性;二是对各地人工智能先行先试立法中的有益经验进行总结,以便从更高效力层次实现人工智能监管的立法供给;三是对人工智能产业发展中遇到的重大难题进行回应,如人工智能的法律责任、人工智能合规义务等,以便凸显人工智能立法的实践特色和发展导向。

然而,需要注意的是,人工智能法不同于人工智能立法,不能期待通过制定一部人工智能法来解决人工智能产业发展遇到的所有难题。首先,古往今来,从来没有一次法典编纂可以完美地囊括其所处社会和时代所需要的全部民事法律规范<sup>[2]</sup>。即使如《中华人民共和国民法典》等成熟已久的立法尚且需要大量留白,考虑到科技发展的日新月异,人工智能法更是无法面面俱到。其次,人工智能法横跨公法与私法,在立法的基本范畴方面仍然有待凝聚共识。加上产业发展的需要、立法资源的联动等各方面原因,未来人工智能法很可能采取“宜粗不宜细”的立法路径,由此留下诸多未决事宜。最后,人工智能本身是一个层次丰富的概念,存在智能科技、智能要素、智能应用三个层面的理解,一部人工智能法难以涵盖所有层次<sup>[3]</sup>。基于此,人工智能法需要平衡好表白与留白的问题。

## 二、人工智能法与智能要素立法的补白

人工智能并非新近产生的技术,而是有着近

70年的发展历史,其间多次经历热潮与低谷。学界通说认为,算法、算力、数据智能三要素的加持,是引发新一轮人工智能热潮的根本原因,也使得人工智能真正得以应用。

2020年8月,美国安全和新兴技术研究中心发布报告《人工智能三要素以及对国家安全战略的意义》指出:“可以用一句话来概括现代人工智能的复杂性,即机器学习系统使用计算能力来执行从数据中学习的算法。”这一定义表明,实现人工智能的关键在于算法、算力、数据三要素。从这个角度来看,人工智能法必然离不开智能要素立法的补白。

欧盟非常关注智能要素的立法,以数据为例。《欧洲数据战略》明确指出:“过去几年,数字技术已经改变了经济和社会,影响了所有的活动领域和欧洲人的日常生活。而数据处于这场转变的中心,并且还会有更多的改变。对企业而言,数据是开发人工智能产品和服务必不可少的资源。”基于此,欧盟《人工智能法》特别强调与数据要素立法的留白与补白。一方面,欧盟《人工智能法》对于数据和数据治理作了明确规定,强调训练数据的合规、个人数据的保护等,以便保障人工智能系统的安全可靠;另一方面,欧盟《人工智能法》特别强调本法无意影响有关个人数据处理的现行欧盟法律的适用,数据权利救济系列问题需要适用欧盟《通用数据保护条例》等数据立法。

中国方面,两部人工智能法建议稿也充分体现了智能三要素的重要性,无论是《人工智能法(学者建议稿)》,还是《人工智能示范法2.0(专家建议稿)》,在人工智能促进与支持专章部分,基本是按照算法、算力、数据三要素来展开的。对此,未来人工智能法需要处理好与智能要素立法的关系。一方面,人工智能法作为对已有数字立法的一次回顾与整理,应将现行智能要素立法的有益经验加以归纳,从人工智能的角度进行规定;另一方面,人工智能法坚持有所为有所不为,对于目前尚未达成共识的问题要敢于留白,如数据财产权,同时留好接口,等待未来智能要素立法的补白。

## 三、人工智能法与智能应用立法的补白

智能要素立法从内部层面很好地补足了人工智能法的留白问题。与此同时,还需要注意,人工

智能具有明显的外溢性特征,即人工智能作为一种赋能型、通用型技术,可以广泛适用于各行各业,包括医疗、教育、金融、消费、交通、制造等,由此产生不同的人工智能应用场景。必须承认的是,各种人工智能应用引发的法律挑战并不完全一样,如自动驾驶汽车关注事故责任问题、人脸识别关心数据合规问题、生成式人工智能则面临著作权保护问题。由此,人工智能法必须考虑智能应用立法问题。

国外方面,智能应用立法受到了广泛关注。以自动驾驶汽车为例,德国出台了《道路交通安全法第八修正案》《自动驾驶法案》,英国制定了《自动化与电动化汽车法案》,韩国发布了《促进和支持自动驾驶汽车商业化法》《促进和支持自动驾驶汽车商业化法施行规则》《促进和支持自动驾驶汽车商业化法施行令》等一系列法案。

国内方面,中央层面发布了《自动驾驶汽车运输安全服务指南(试行)》《关于开展智能网联汽车准入和上路通行试点工作的通知》;地方层面也纷纷出台了各种道路测试规则,如深圳出台了全国首部自动驾驶汽车的地方性法规《深圳经济特区智能网联汽车管理条例》,上海出台了《上海市浦东新区促进无驾驶人智能网联汽车创新应用规定实施细则》。

当然,考虑到人工智能应用场景十分丰富,有关智能应用的立法还远远没有完成,需要日后通过持续的立法来予以更新。对此,人工智能法需要充分协调与智能应用立法的关系。一方面,人工智能法在总分结构的统摄安排下,可以考虑设置特殊人工智能应用场景专章,以便将典型人工智能应用场景的典型问题提出来,以一般法的形式进行明确,为未来智能应用的立法提供指导。对此,《人工智能法(学者建议稿)》提炼了行政人工智能、司法人工智能、新闻人工智能、医疗人工智能、社交机器人、生物识别、自动驾驶汽车、社会信用人工智能以及通用人工智能9个应用场景的典型问题。另一方面,人工智能法也需要为智能应用立法的补白留下接口,对于人工智能开发者、提供者、使用者的权利义务责任,人工智能产品或者服务的准入与监管,都需要通过“法律另有规定”的引致条款留有余地。

——郑志峰(西南政法大学科技法学研究院教授)

## 参考文献:

- [1] 张凌寒.中国需要一部怎样的《人工智能法》?——中国人工智能立法的基本逻辑与制度架构[J].法律科学,2024,42(3):3—17.
- [2] 张力.中国民法典编纂:目标、任务与路径[J].中国经济报告,2016(8):12—15.
- [3] 郑志峰.人工智能立法的一般范畴[J].数字法治,2023(6):55—75.

## 人工智能法的调整范围

人工智能法的调整范围是人工智能立法最核心的核心议题之一。人工智能法,不仅需要划定哪些对象和哪些行为受该法调整,而且应当明确规定哪些行为排除在该法调整范围之外。该问题的回答与人工智能法的定位以及基本范畴的界定紧密相连,并将显著影响人工智能法的立法效果。

### 一、由立法目的设定调整范围

人工智能法立法目的应当兼顾发展与安全。一方面,促进人工智能发展早已成为国家规划的一部分。2017年,国务院《新一代人工智能发展规划》提出了“到2030年人工智能理论、技术与应用总体达到世界领先水平”的目标。发展人工智能的根本目的更在于,促进经济高质量发展,服务数字中国建设。另一方面,中国历来重视防范人工智能风险。2023年4月28日,习近平在主持召开中共中央政治局会议时指出:“要重视通用人工智能发展,营造创新生态,重视防范风险。”<sup>[1]</sup>由此出发,中国人工智能立法目的,既在于推动人工智能技术创新,促进人工智能产业健康发展,又在于规范人工智能产品和服务的开发、提供、使用活动及其监督管理,维护国家安全和公共利益,保护个人及组织的合法权益。

不难看出,人工智能法立法目的之中已然蕴含了调整范围。与欧盟法上“投放市场或投入使用”的限定不同,中国人工智能法应当坚持人工智能的全链条、全流程控制。投入流通是产品责任的限制条件,而非科技创新与监管的限制。从中国相关制度来看,《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《科技伦理审查办法(试行)》等法律法规均采取全流程规制的方法。人工智能法应当将人工

智能产业链的各个环节全面列入调整范围,不仅包括人工智能的提供者,还包括开发者与使用者,由此实现从源头到终端的治理。此外,人工智能的应用及其后果是跨越国界的,人工智能法应当采取保护管辖原则,凡是可能影响中国国家安全、公共利益或者个人及组织合法权益的,都应当被纳入调整范围。欧盟《人工智能法》亦规定了域外效力条款,只要是人工智能“产生的产出用于欧盟”则适用该法。在此认识的基础上,人工智能法的调整范围也应当坚持发展导向,合理界定基本范畴以及设定排除条款,为人工智能法划定边界。

## 二、以基本范畴限定调整范围

通过界定何谓人工智能,可以有效地将人工智能法的调整范围与传统科技创新和网络立法的调整范围相区分。自1956年达特茅斯会议上人工智能的概念被提出以来,人工智能经历了“三起三落”,至今已发展成为一门独立的学科。该学科主张,人工智能是指用计算机模拟人类智能行为的科学。然而,若采取这一定义,则许多自动化系统也可能被纳入人工智能的范畴,这将模糊人工智能法的调整对象。针对此问题,人工智能立法中宜采取“目的+行为+用途”定义,将人工智能界定为:为了实现专用或者通用目的,利用计算机模拟人类智能行为,用于预测、建议、决策或者生成内容等用途的技术。

需要注意的是,人工智能本身作为一种技术,不能成为人工智能法的调整对象。原因在于,法律只能调整人的行为,而不能调整技术本身。与人工行为发生关联的应该是人工智能产品和服务。虽然受国家网信办职能的限制,以《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理暂行办法》为代表的法规针对的是人工智能服务,但是并不能因此排除人工智能法对产品的关注。自动驾驶汽车、手术机器人等即属于典型的人工智能产品。人工智能法必须广泛关注智能科技的多维应用。

此外,人工智能法的调整对象不宜通过人工智能的要素进行拆分。通常认为,人工智能具有算法、算力、数据三要素,网络、场景要素也时常被提及作为第四要素和第五要素。若将人工智能法简单拆分为关于人工智能要素的立法,则会消解人工

智能法的立法目的,而且还会模糊人工智能法与网络法的关系<sup>[2]</sup>。也就是说,智能科技、智能要素均不是人工智能法的调整对象,人工智能法只调整人工智能产品和服务的开发、提供、使用活动。

## 三、调整范围的例外

为了在人工智能法中兼顾发展与安全,在人工智能产品和服务的开发、提供、使用活动中,应当设置以下四种例外。

首先,在开发活动中排除纯粹的科学研究活动。开发不等同于研发。研发是研究与开发的统称。有学者主张,“人工智能技术研发活动”是人工智能法的调整对象,包括“科学研究、技术开发和产品研制等活动”<sup>[3]</sup>。然而,若将纯粹的科研活动纳入调整范围,则大量高校实验室需要承担人工智能法的风险评估、数据质量等义务,这将阻碍人工智能科技创新。因此,应当仅将以提供人工智能产品为目的的开发活动作为调整对象,若产品和服务最终流向第三方或社会公众,则开发活动受到监管;反之,若仅仅是人工智能的科学研究,未形成产品和服务,则属于不受人工智能法调整的科学研究活动。

其次,在提供活动中排除免费开源的提供行为。开源模型的提供者实际上难以有效约束二次利用活动,而开源生态又是人工智能产业的重要组成部分。人工智能立法应当旗帜鲜明地支持相关主体建设或者运营开源平台、开源社区、开源项目,鼓励企业开放软件源代码、硬件设计、应用服务,培育共享协作的开源创新生态。在基础模型的法律责任中,开源模型应当相应地获得豁免。若对免费开源的人工智能提供者施加额外的义务,则必将对开源生态造成打击,不利于人工智能产业的发展。

再次,在使用活动中应当排除自然人因个人或者家庭事务使用人工智能的情形。《中华人民共和国个人信息保护法》第72条第1款即规定了家事处理的例外,欧盟《人工智能法》亦排除了“个人非职业活动中使用人工智能系统”的情形。数字社会中,个人事务使用人工智能的情形较为普遍,不仅智能家居设备已经走进了千家万户,而且个人还可以对大模型进行训练以满足其个性化需求。人工智能法应当重点调整的是数字能力不对等的关系,



个人家庭事务行为则受《中华人民共和国民法典》调整。

最后,人工智能的军事开发利用活动,难以全面履行人工智能法的各项义务,更不可能直接向行政部门报告或直接接受人工智能监管部门的监管,因此相关规则应当另行规定。

基于上述认识,人工智能法的调整范围应规定为在中国境内从事人工智能开发、提供、使用活动及其监督管理,以及在中国境外开展人工智能开发、提供、使用活动,可能影响中国国家安全、公共利益或者个人及组织合法权益的情形。同时,针对科学研究、免费开源提供、个人或家事使用、军事开发利用四类情形设置除外条款。

——韩旭至(华东政法大学数字法治研究院副院长、副教授)

#### 参考文献:

- [1] 中共中央政治局召开会议 分析研究当前经济形势和经济工作中 央总书记习近平主持会议[N]. 人民日报, 2023-04-29(1).
- [2] 陈亮. 人工智能立法体系化的困境与出路[J]. 数字法治, 2023(6): 10—17.
- [3] 侯东德. 人工智能法的基本问题及制度架构[J]. 政法论丛, 2023(6): 61—72.

## 人工智能立法体系的三类要素

ChatGPT的面世标志着人工智能技术发展迈向全新阶段,这也引发了学界关于是否有必要进行人工智能立法的大讨论。从目前主流观点来看,多数学者倾向在《互联网信息服务算法推荐管理规定》《生成式人工智能服务暂行管理办法》等现行法律法规的基础上,结合 ChatGPT、Sora 等人工智能产品实践现状,制定专门的人工智能法,并且不少学者也提出了不同版本的人工智能法草案。然而,值得注意的是,在技术安全风险预防成为人工智能治理核心内容的研究趋势下,人工智能立法不能仅仅停留于安全风险预防层面,更应当以更加多元化的视角建构促进科技创新、技术风险预防等目标在内的综合性立法体系,并以算法、算力、数据的供给保障作为具体规则的核心内容。

## 一、立法体系要素之一: 风险预防

现阶段,人工智能立法具体规则的大部分内容是围绕风险预防展开的,相应的制度内容也延伸出既有法律规则的解释适用与新兴法律规则的创设建构两大内容。事实上,当 Sora、Claude 等更加强大的生成式人工智能产品出现之后,相应的技术风险也趋于稳定化和类型化,未能产生远超立法者想象的技术效果。技术风险的相对确定性也使得相应的立法重心变为“如何建构体系化的统一监管立法”,其核心的论证要素依然是“技术风险”和“安全保障”。在某种程度上,风险预防已经成为人工智能法学研究领域的“通用范式”,不少学者在各自的制度建构主张中也将“风险预防”或者“安全保障”作为法律基本原则之一。尽管“风险”与“安全”二词时常在数字法学研究中同时出现,但二者并非二元对立关系,与“风险”相关的法律价值还包括“可信”。在“没有绝对安全的技术”的共识基础上,法律对于技术风险的治理效果开始强调基于“相对安全”形成社会公众对技术应用的信任,以此实现技术创新的普及应用。

## 二、立法体系要素之二: 科技创新激励

人工智能立法的首要立法目标是促进人工智能科技创新,而这一点往往被学界所忽视。诚然,风险预防范式确实能够推动人工智能产业依循着更加合理的方向进行创新,但这终归是间接促进的方式。促进科技创新最为直接有效的方式是遵循“市场调节为主,政府干预为辅”的治理逻辑,通过保障科技创新主体的合法权益、推动科技成果转化等方式实现创新。虽然《中华人民共和国科学技术进步法》等现行立法在科技成果转化、产学研科技合作创新等领域作出了明确规定,但是从基础理论创新到成果商业应用这一转化过程来看,不同领域的技术创新还需要专门的制度规范。一方面,人工智能立法应当着眼于市场自发调节的客观规律和要素特征,以市场调节主导的方式提升科技创新的经济动因;另一方面,人工智能立法应当厘清科技行政管理、科技成果评价等方面存在的制度障碍,



为科技创新提供必要的制度保障。

### 三、立法体系要素之三： 创新资源保障

市场调节固然可以最大化地实现科技创新的经济激励效应,但市场调节不可避免地会存在失灵现象,此时就需要政府部门介入,保障人工智能科技创新的要素供给。在人工智能立法中,创新要素供给实际上也是围绕算法、算力、数据三大创新要素予以展开,其目标也在于预防三类科技创新效率现象的发生。其一,一旦市场不存在同类竞品或更优质产品,创新主体在短时间内反而缺少科技创新的经济动机;其二,持有优质产品的创新主体存在海量用户时,可能会借由用户规模优势研发与一般产品兼容的次等产品,用以抢占次等产品市场竞争中的创新资源;其三,部分创新资源属于公共物品,完全交由市场调节可能会使得在后的市场主体采用各种方式阻碍在后的市场主体获取相同的创新资源。

### 四、基于三类立法体系要素的 方法论

在促进人工智能技术创新方面,风险预防、科技创新激励和创新资源保障三类立法体系,实际上对应了安全可靠原则、经济效益原则和基础设施保障原则三项人工智能立法的方法论。

安全可靠原则是指人工智能技术研发和应用应当满足能够确保技术安全风险控制在可接受范围。具体而言,安全可靠原则包括三个要素:一是

符合安全技术标准和法定安全管理义务。人工智能技术的创新方式应当符合法律法规有关技术安全保障的强制性规定,同时,在具体应用场景中,应当优先采用符合通用安全技术标准的技术架构、通信协议。二是既能够有效预防常见的技术安全风险,也能够网络安全事件中快速恢复基本功能。三是符合科技伦理审查要求。人工智能技术的应用方式理应以保护人格尊严和自由为基础,在设计研发、商业应用等各个科技创新环节进行科技伦理审查。

经济效益原则是指人工智能技术创新的促进机制应当符合市场经济效益要求,技术创新鼓励性条款、促进性条款应当着重强调“市场调节为主导,政府干预为辅助”的基本要求,衔接好市场调整机制与政府干预机制促进人工智能技术创新的功能定位。

基础设施保障原则是指人工智能技术创新的促进机制应当包含人工智能技术创新所必需的创新资源供给。目前,算法、算力、数据已成为影响人工智能技术创新的核心三要素,相应的创新资源供给机制也应当围绕这三要素予以建构。例如,在算法层面,市场激励机制不可能实现直接由市场提供基础技术的创新,这种失灵现象则需要在制度层面明确政府促进科技创新的法定职责,既需要鼓励和支持高等院校、科研机构开展基础算法模型的科研攻关,也需要有规划地培养基础算法模型领域的关键人才。

——赵精武(北京航空航天大学法学院副教授)、周瑞珏(北京航空航天大学计算机学院博士后)