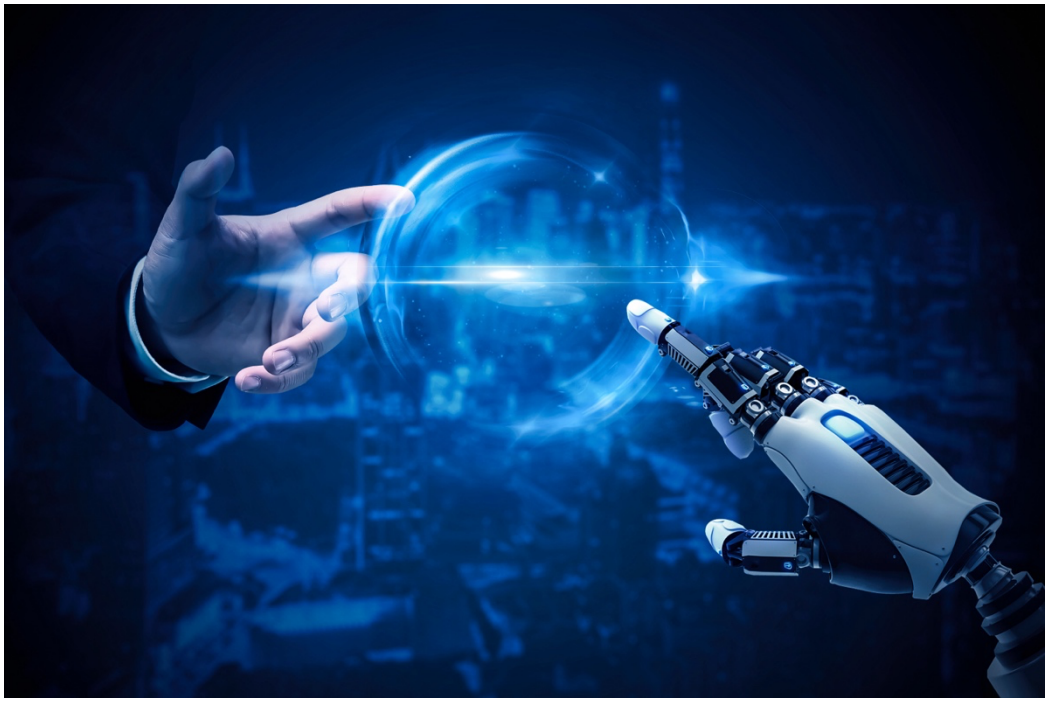
中国人民大学法学院
数字法学教研月报

2024 年第 10 期（总第 10 期） 2024 年 10 月 20 日



【数字法治大事件】近期，中国在数字法治领域采取了一系列重要措施，包括国家数据局对个人信息保护的严格要求、《数据领域名词解释》的公众意见征集、《人工智能能力建设普惠计划》的提出，以及《网络数据安全管理条例》的公布等。五部门联合出台的《个人求助网络服务平台管理办法》进一步规范了个人求助网络服务平台的运营，保护了捐助资金的安全和管理。国家发改委、国家数据局等部门联合印发的《国家数据标准体系建设指南》为数据标准化工作提供了全面指导，推动构建以数据为关键要素的数字经济。网络与信息法学会 2024 年年会暨第二届数字法治大会、第二届数字法治大会分论坛在云南昆明圆满闭幕。《数据产权论》新书发布会在清华大学成功举办。

【研究动态】近期发表的数字法学的相关研究展示了数字技术对法律体系和治理结构日益增长的影响。研究的重点领域包括为应对现代技术（如数据、算法和信息风险）带来的复杂跨学科挑战而演变的数字立法。学者们深入探讨了技术与治理的交叉点，研究人工智能对立法过程、问责制及权力失衡的影响。数字隐私、个人数据保护以及对人工智能和数字平台的监管也是核心主题，法律框架正在更新，以反映这些领域中不断变化的风险和责任。

【教研活动】中国人民大学法学院“新科技革命与未来法治创新团队”入选“教育部哲学社会科学创新团队建设名单”。张新宝教授应邀为云南大学法学院师生作主题为“数字法学基本问题”讲座。

【数字法评】《赋能型人工智能治理的理念确立与机制》，《中国法学》2024 年第 5 期，作者张吉豫。《论人工智能立法的基本路径》，《中国法学》2024 年第 5 期，作者林洹民。

本期目录

数字法治大事件

李强签署国务院令 公布《网络数据安全管理条例》

原载: “网信中国”微信公众号

国务院总理李强日前签署国务院令，公布《网络数据安全管理条例》（以下简称《条例》），自2025 年 1 月 1 日起施行。

《条例》旨在规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。《条例》共 9 章 64 条，主要规定了以下内容。

一是提出网络数据安全管理总体要求和一般规定。明确鼓励网络数据在各行业、各领域的创新应用，对网络数据实行分类分级保护，积极参与网络数据安全相关国际规则和标准的制定，加强行业自律，禁止非法网络数据处理活动。要求网络数据处理者履行建立健全网络数据安全管理制度、安全风险报告、安全事件处置等义务。

二是细化个人信息保护规定。明确处理个人信息的规则和应当遵守的具体规定。要求网络数据处理者提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。明确使用自动化采集技术等采集个人信息的保护义务，细化个人信息转移请求实现途径等。

三是完善重要数据安全制度。明确制定重要数据目录职责要求，规定网络数据处理者识别、申报重要数据义务。规定网络数据安全管理机构和网络数据安全负责人的责任。明确重要数据风险评估具体要求。

四是优化网络数据跨境安全管理规定。明确网络数据处理者可以向境外提供个人信息的条件，规定可以按照缔结或者参加的国际条约、协定向境外提供个人信息。规定未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。

五是明确网络平台服务提供者义务。规定网络平台服务提供者、第三方产品和服务提供者等主体的网络数据安全保护要求。明确通过自动化决策方式向个人进行信息推送的规则，规定大型网络平台服务提供者发布个人信息保护社会责任年度报告、防范网络数据跨境安全风险等要求。

五部门出台《个人求助网络服务平台管理办法》

原载: 百度网百家号“央视新闻”

民政部、国家网信办、工业和信息化部、公安部、金融监管总局今天（9 月 5 日）联合公布《个人求助网络服务平台管理办法》，自公布之日起施行。

《个人求助网络服务平台管理办法》主要内容有：

（一）关于《办法》规制的范围。《办法》规制的是专门为因疾病等原因导致家庭经济困难的个人，提供求助信息发布和捐助资金归集、管理、拨付等服务的网络平台。《办法》规定，个人求助网络服务平台，应当经民政部指定；未经指定，任何组织或者个人不得以个人求助网络服务平台的名义开展活动，不得从事求助信息发布和捐助资金归集、管理、拨付等个人求助网络服务。

（二）关于个人求助网络服务平台的指定。申请指定为个人求助网络服务平台的，应当符合本《办法》第四条规定的条件，并提交相关材料。民政部将根据工作安排，发布遴选个人求助网络服务平台的公告；组建评审委员会，确定拟指定的个人求助网络服务平台名单，并向社会公示；公示期满后，确定指定的个人求助网络服务平台名单并向社会公布。 名单公布后，个人求助网络服务平台应当在六十日内提供服务。

（三）关于个人求助网络服务平台的主要规则。服务协议、求助信息发布规则、个人信息处理规则等平台规则文件是保护用户合法权益、维持平台健康有序运营的基础。《办法》在申请指定条件中明确要求平台已制定健全的平台规则文件；对平台规则进行重大调整的，应当在调整前向民政部报告；

平台应当在求助人、信息发布人、捐助人同意平台规则以及捐助资金使用、退回等约定后，再向其提供服务。《办法》还明确了平台要遵守的原则和信息内容管理、信息安全管理、个人信息保护等方面的要求。平台、求助人、信息发布人、捐助人之间的纠纷，可以通过自行和解、向仲裁机构申请仲裁、向人民法院提起诉讼等途径解决。

（四）关于求助信息的真实性查验。对求助信息的真实性进行查验是个人求助网络服务平台的法定义务，《办法》从个人求助网络服务平台、求助人、信息发布人等多个角度进行了规定：

一是在申请指定条件中明确平台需具备查验通过其发布的求助信息真实性的能力。

二是规定平台应当明确告知求助人、信息发布人对求助信息的真实性负责，明确告知求助人、信息发布人不得通过虚构、隐瞒事实等方式骗取救助。

三是明确了求助人、信息发布人需要提交的求助信息和相关材料；规定平台应当建立审核团队，对求助信息的真实性进行查验。

四是规定平台查验求助信息的真实性后，应当及时向社会公开相关信息，接受社会监督。

五是规定平台发现求助人、信息发布人涉嫌诈骗等犯罪行为的，应当及时向公安机关反映。

（五）关于对捐助资金的管理要求。捐助资金的安全和管理是《办法》规制的重点内容：

一是在申请指定条件中明确要求平台的运营主体与银行签订捐助资金存管协议。

二是规定平台归集的捐助资金应当由专用存款账户管理、专项使用，并对捐助资金专用存款账户的开设问题作出了规定。

三是规定除平台收取服务费用、捐助资金无法原路退回等情形外，专用存款账户归集的捐助资金只能向求助人本人或者其提供的医院账户等转账。

四是规定平台应当承担捐助资金拨付审核责任，建立审核机制，加强对捐助资金拨付的审核，并及时向求助人拨付捐助资金；应当监督求助人按照求助用途使用捐助资金，要求求助人、信息发布人及时更新捐助资金使用情况。

五是明确了平台要求相关责任人退回捐助资金并退还捐助人的情形。

六是规定平台应当及时、全面向社会公开每个求助人相关的资金筹集、拨付、使用、退回等信息，便于社会各界监督。

（六）关于对个人求助网络服务平台的监督管理。民政部、国家网信办、工业和信息化部、公安部、金融监管总局等部门，将协同加强对个人求助网络服务平台的监督管理：

一是规定平台于每年 6 月 30 日前向民政部报送上一年度工作报告和财务会计报告；每半年向社会公开一次其从事个人求助网络服务的情况。

二是明确了相关部门对涉嫌违反本《办法》规定的平台及其运营主体，有权按照法定职责采取的监管措施。

三是平台及其运营主体涉嫌违反《办法》规定的，相关部门可以对有关负责人进行约谈，要求其说明情况、提出改进措施。

（七）关于个人求助网络服务平台的法律责任。根据行政处罚法和有关法律法规，《办法》明确了个人求助网络服务平台的法律责任：

一是平台及其运营主体违反本《办法》规定的，由民政部、国家网信办、工业和信息化部、公安部、金融监管总局等部门按照法定职责责令限期改正，予以警告或者通报批评。

二是平台的工作人员违反本《办法》第二十条规定，构成违反治安管理行为的，由公安机关依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

三是规定了平台取消指定的五种情形，并明确了对被取消指定平台的后续工作要求。此外，对未经指定的互联网信息服务提供者擅自以个人求助网络服务平台的名义开展活动或者从事个人求助网络服务的，由县级以上人民政府民政部门责令限期改正；逾期不改正的，由县级以上人民政府民政部门会同网信、电信主管部门依法进行处理。

（总台央视记者 李玉梅）

全文丨国家发改委、国家数据局等部门联合印发《国家数据标准体系建设指南》

原载：“数据要素社”微信公众号

10 月 8 日，国家发展改革委、国家数据局、中央网信办、工业和信息化部、财政部、国家标准委联合印发《国家数据标准体系建设指南》（以下简称《建设指南》）。

《建设指南》深入贯彻落实习近平总书记关于数据发展和安全的重要论述精神，以数据“供得出、流得动、用得好、保安全”为指引，从基础通用、数据基础设施、数据资源、数据技术、数据流通、融合应用、安全保障等 7 个部分，加快构建数据标准体系，全面指导数据标准化工作开展，为制修订数据领域相关标准提供了重要指引，有利于充分发挥数据标准体系在激活数据要素潜能、建设数据产业生态、做强做优做大数字经济、培育和发展新质生产力等方面的引领和规范作用。

《建设指南》提出计划到 2026 年底，基本建成国家数据标准体系，围绕数据流通利用基础设施、数据管理、数据服务、训练数据集、公共数据授权运营、数据确权、数据资源定价、企业数据范式交易等方面，制修订 30 多项数据领域基础通用国家标准，形成一批标准应用示范案例，建成标准验证和应用服务平台，培育一批具备数据管理能力评估、数据评价、数据服务能力评估、公共数据授权运营绩效评估等能力的第三方标准化服务机构。

下一步，国家发展改革委、国家数据局和有关部门将强化组织保障、增强协同合力，深化贯标验证，发挥应用成效，加强人才培养，筑牢发展根基，确保数据标准化工作落到实处，推动构建以数据为关键要素的数字经济，有效发挥数据的基础资源作用和创新引擎作用。

政策原文

各省、自治区、直辖市及计划单列市、新疆生产建设兵团发展改革委、数据管理部门、党委网信办、工业和信息化主管部门、财政厅（局）、市场监管局（厅、委）：

为深入学习贯彻党的二十大和二十届二中、三中全会精神，落实《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》要求，充分发挥标准在激活数据要素潜能、做强做优做大数字经济等方面的规范和引领作用，国家发展改革委、国家数据局、中央网信办、工业和信息化部、财政部、国家标准委组织编制了《国家数据标准体系建设指南》。现印发给你们，请各地区、各行业结合实际，抓好落实。

国家发展改革委

国家数据局

中央网信办

工业和信息化部

财政部

国家标准委

2024 年 9 月 25 日

国家数据局：涉个人信息的公共数据要进行脱敏和匿名化处理

原载：央视新闻客户端

在今天国务院新闻办公室举行的新闻发布会上，国家数据局有关负责人表示，**国家将严格管控未依法依规公开的原始公共数据直接进入市场，严禁运营机构未经授权超范围使用数据。**

国家数据局有关负责人介绍说，《意见》明确，运营机构要切实履行数据安全的主体责任，采取必要措施，保障数据安全。特别是对于其中涉及个人信息的公共数据，要严格落实《个人信息保护法》，进行脱敏和匿名化处理，避免侵犯个人的信息权益。鼓励开发数据模型、数据核验、评价指数等形式的数据产品，实现“原始数据不出域，数据可用不可见”。

国家数据局数据资源司司长 张望：我们将支持数据加密、可信流通、安全治理等技术创新和应用，更好地解决数据利用中的安全问题。

（总台央视记者 刘颖 刘柏煊 陈茜）

关于向社会公开征求《数据领域

名词解释》意见的公告

原载：“国家数据局”微信公众号

为进一步凝聚共识，推动社会各界对数据领域术语形成统一认识，现就《数据领域名词解释》向社会公开征求意见。

此次征求意见的时间是 2024 年 10 月 21 日至 11 月 20 日。欢迎社会各界人士提出意见，请通过电子邮件方式将意见发送至 gjsjjzcs@126.com

感谢您的参与和支持！

附件：数据领域名词解释

数据领域名词解释起草专家组

2024 年 10 月 21 日

附件

数据领域名词解释

1. 数据。是指任何以电子或其他方式对信息的记录。数据在不同视角下表现为原始数据、衍生数据、数据资源、数据产品、数据资产、数据要素等形式。

2. 原始数据。是指初次或源头收集的、未经加工处理的数据。

3. 数据资源。是指具有使用价值的数据，是可供人类利用的新型资源。

4. 数据要素。是指能直接投入到生产和服务过程中的数据，是用于创造经济或社会价值的新型生产要素。

5. 数据产品。是指基于数据加工形成的，可满足特定需求的数据加工品和数据服务。

6. 数据资产。是指特定主体合法拥有或者控制的，能进行货币计量的，且能带来直接或者间接经济利益的数据资源。

7. 数据要素市场化配置。是指通过市场机制来配置数据这一新型生产要素，旨在建立一个更加开放、安全和高效的数据流通环境，不断释放数据要素价值。

8. 数据处理。包括数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

9. 数据处理者。是指在数据处理活动中自主决定处理目的和处理方式的个人或者组织。

10. 受托数据处理者。是指接受他人委托处理数据的个人或者组织。

11. 数据流通。是指数据在不同主体之间流动的过程，包括数据开放、共享、交易、交换等。

12. 数据交易。是指数据供方和需方之间进行的，以数据或者数据各类形态为标的的交易行为。

13. 数据交互。是指主体之间以数据的形式进行交流和协作的过程。

14. 数据治理。是指提升数据的质量、安全、合规性，推动数据有效利用的过程，包含组织数据治理、行业数据治理、社会数据治理等。

15. 数据安全。是指通过采取必要措施，确保数据处于有效保护和合理利用的状态，以及具备保障持续安全状态的能力。

16. 公共数据。是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。

17. 数字产业化。是指新一代移动通信、人工智能等数字技术向数字产品、数字服务转化，数据向资源、要素转化，形成数字新产业、新业态、新模式的过程。

18. 产业数字化。是指传统的农业、工业、服务业等产业通过应用数字技术、采集融合数据、挖掘数据资源价值，提升业务运行效率，降低生产经营成本，进而重构思维认知，整体性重塑组织管理模式，系统性变革生产运营流程，不断提升全要素生产率的过程。

19. 数字经济高质量发展。围绕加快培育新质生产力，以数据要素市场化配置改革为主线，协同完善数据基础制度和数字基础设施，全面推进数字技术和实体经济深度融合，持续提升数字经济治理能力和国际合作水平，实现数字技术革命性突破、数据要素创新性配置、传统产业数字化转型和适数化改革，通过数字经济创新发展赋能经济社会高质量发展。

20. 数字消费。是指数字新技术、新应用支撑形成的消费活动和消费方式，既包括对数智化技术、产品和服务的消费，也包括消费内容、消费渠道、

消费环境的数字化与智能化，还包括线上线下深度融合的消费新模式。

21.产业互联网。是指利用数字技术、数据要素推动全产业链数据融通，赋能产业数字化、网络化、智能化发展，推动业务流程、组织架构、生产方式等重组变革，实现产业链上下游协同转型、线上线下融合发展、全产业降本增效与高质量发展，进而形成新的产业协作、资源配置和价值创造体系。

22.城市全域数字化转型。是指城市以全面深化数据融通和开发利用为主线，综合利用数字技术应用和制度创新工具，实现技术架构重塑、城市管理流程变革和产城深度融合，促进数字化转型全领域增效、支撑能力全方位增强、转型生态全过程优化的城市高质量发展新模式。

23.“东数西算”工程。是把东部地区经济活动产生的数据和需求放到西部地区来计算和处理，对数据中心在布局、网络、电力、能耗、算力、数据等方面进行统筹规划的重大工程，比如人工智能模型训练推理、机器学习等高时延业务场景，可以通过“东数西算”的方式让东部业务向西部风光水电丰富的区域迁移，实现东西部协同发展。加快推动“东数西算”工程建设，将有效激发数据要素创新活力，加速数字产业化和产业数字化进程，催生新技术、新产业、新业态、新模式，支撑经济高质量发展。

24.高速数据网。是指面向数据流通利用场景，依托网络虚拟化、软件定义网络（SDN）等技术，提供弹性带宽、安全可靠、传输高效的数据传输服务，具有高带宽、低延迟、高可靠性、高安全性、可扩展性、灵活性等特点。

25.全国一体化算力网。是指以信息网络技术为载体，促进全国范围内各类算力资源高比例、大规模一体化调度运营的数字基础设施。作为“东数西算”工程的 2.0 版本，具有集约化、一体化、协同化、价值化四个典型特征。

26.元数据。关于数据或数据元素的数据（可能包括其数据描述），以及关于数据拥有权、存取路径、访问权和数据易变性的数据。

27.结构化数据。一种数据表示形式，按此种形式，由数据元素汇集而成的每个记录的结构都是一致的并且可以使用关系模型予以有效描述。

28.半结构化数据。不符合关系型数据库或其他数据表的形式关联起来的数据模型结构，但包含相关标记，用来分隔语义元素以及对记录和字段进行分层的一种数据化结构形式。

29.非结构化数据。是指不具有预定义模型或未以预定义方式组织的数据。

30.数据分析。是指利用技术手段，对数据进行分析，发挥数据作用、释放数据价值的过程。

31.数据挖掘。是数据分析的一种手段，是从大量数据中通过算法搜索隐藏于其中信息的过程。

32.数据可视化。是指将数据以图表、图形、地图等可视化形式展示，以便更好地理解和分析数据。

33.数据仓库。是指一个面向主题的、集成的、相对稳定的、反映历史变化的数据集合，通常用于支持企业或组织的决策分析处理。

34.数据湖。是指一种高度可扩展的数据存储架构，它专门用于存储大量原始数据，这些数据可以来自各种来源并以不同的格式存在，包括结构化、半结构化和非结构化数据。

35.湖仓一体。是指一种新型的开放式的存储架构，打通了数据仓库和数据湖，将数据仓库的高性能及管理能力与数据湖的灵活性融合起来，底层支持多种数据类型并存，能实现数据间的相互共享，上层可以通过统一封装的接口进行访问，可同时支持实时查询和分析，为企业进行数据治理带来了更多的便利性。

36.隐私计算。是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私计算的常用技术方案有多方安全计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

37.多方安全计算。是指在无可信第三方的条

件下，通过特殊设计的密码学算法和协议，允许多个参与方在不泄露各自隐私数据的前提下，协同完成计算任务。

38.联邦学习。是指多个参与方在不共享原始数据的情况下协作完成机器学习任务的方法。

39.可信执行环境。是指提供基于硬件级的系统隔离和可信根，支持基于技术信任的数据安全保障能力，保证在安全区域内部加载的代码和数据在保密性和完整性方面得到保护。

40.密态计算。是指通过综合利用密码学、可信硬件和系统安全的可信隐私计算技术，其计算过程实现数据可用不可见，计算结果能够保持密态化，以支持构建复杂组合计算，实现计算全链路保障，防止数据泄漏和滥用。

41.区块链。是指使用密码链接将共识确认的区块按顺序追加形成的分布式账本。

速览！中方宣布《人工智能能力建设普惠计划》

原载：“中国网信杂志”微信公众号

当地时间 9 月 25 日，“人工智能能力建设国际合作高级别会议”在纽约联合国总部举行。中方在会上提出《人工智能能力建设普惠计划》，引起国际社会广泛关注和积极支持。

人工智能能力建设普惠计划

为弥合数字和智能鸿沟，特别是帮助全球南方在人工智能发展进程中平等受益，中方认为要坚持联合国在国际发展合作中的统筹协调作用，坚持真正多边主义，基于主权平等、发展导向、以人为本、普惠包容、协同合作原则，通过南北合作、南南合作和三方合作等形式，切实落实联大加强人工智能能力建设国际合作决议（A/RES/78/311），推动落实联合国 2030 年可持续发展议程。为此，中国提出“人工智能能力建设普惠计划”，并呼吁各方对人工智能能力建设加大投入。

一、愿景目标

（一）促进人工智能和数字基础设施联通

完善全球可互操作的人工智能和数字基础设施布局，积极协助各国特别是全球南方发展人工智能技术和服务，助力全球南方真正接触到人工智能，跟上人工智能发展的步伐。

（二）推进“人工智能+”赋能千行百业

探索推进人工智能全方位全链条多场景赋能实体经济，推进人工智能赋能工业制造、传统农业、绿色转型发展、气候变化应对、生物多样性保护等应用，因地制宜推动构建丰富多样、健康向善的人工智能发展生态。

（三）加强人工智能素养和人才培养

积极推动人工智能在教育中的广泛应用，开展人工智能人才培养和交流，加大分享通用专业知识和最佳实践，培育公众人工智能素养，保障和强化妇女和儿童数字和智能权益，共享人工智能知识成果和经验。

（四）提升人工智能数据安全和多样性

合作推动数据依法有序自由跨境流动，探索构建数据共享的全球性机制平台，维护个人隐私和数据安全。推动人工智能数据语料库平等多样，消除种族主义、歧视和其他形式的算法偏见，促进、保护和保全文明多样性。

（五）确保人工智能安全可靠可控

坚持公平和非歧视原则，支持在联合国框架下建立兼顾发展中国家利益的全球可互操作的人工智能安全风险评估框架、标准和治理体系。共同研判人工智能研发与应用风险，积极推进和完善应对人工智能安全风险的技术和政策，确保人工智能设计、研发、使用和应用促进人类福祉。

二、中国行动

（一）中方愿同所有国家开展人工智能领域南北合作、南南合作和三方合作，共同落实联合国未来峰会成果，积极同各国特别是发展中国家开展人工智能基础设施建设合作，共建联合实验室。

（二）中方愿开展人工智能模型研发和赋能合作，特别是推进人工智能赋能减贫、医疗、农业、教育和工业制造等，深化人工智能产供链国际合作，释放人工智能作为新质生产力的红利。

（三）中方愿同各国特别是发展中国家共同挖掘人工智能赋能绿色发展、气候变化应对、生物多样性保护等潜力，助力全球气候治理和可持续发展。

（四）中方愿搭建人工智能能力建设国际合作平台，中方人工智能产业界和产业联盟愿同各国特别是发展中国家开展多种形式的交流活动，共享最佳实践，以负责任态度共建人工智能开源开放社区，推动构建多层次多业态合作生态。

（五）中国政府将面向发展中国家举办人工智能能力建设中短期教育培训，共享人工智能教育资源，开展人工智能联合办学和访问交流等活动，助力发展中国家培养高水平人工智能科技与应用人才。

（六）中国政府愿加强同发展中国家的人力资源援助合作，在今年举办首届人工智能能力建设研讨班的基础上，将于 2025 年底前重点面向发展中国家再举办十期人工智能领域研修研讨项目。

（七）中方愿同各国特别是发展中国家共同培育公众人工智能素养，以线上线下相结合方式，多维度、多层次、多载体推广人工智能科普和专业知识，努力提高各自人民的人工智能素养和技能水平，特别是保障和提高妇女和儿童数字权益。

（八）中方愿同各国特别是发展中国家共同开展人工智能语料建设，采取积极举措消除种族、算法、文化歧视等，致力于维护并促进语言和文明多样性。

（九）中方愿同各国特别是发展中国家促进和完善数据基础设施，共同促进全球数据公平普惠利用。

（十）中方愿同各国特别是发展中国家共同加强人工智能战略对接和政策交流，积极分享在人工智能测试、评估、认证与监管方面的政策与技术实践，携手应对人工智能伦理与安全风险。

央行数研所穆长春：稳妥推进数字人民币研发和应用 扎实助力金融强国战略

原载：“21 财经”App“时事报告”

文/中国人民银行数字货币研究所所长 穆长春

习近平总书记提出加快建设金融强国，强调金融强国具备一系列关键核心金融要素，包括强大的货币、强大的中央银行等。中国人民银行深入贯彻落实习近平总书记关于金融工作的一系列重要论述，把数字人民币工作作为建设强大的货币、强大的中央银行的重要抓手之一，历经理论研究、封闭测试和开放试点，走出一条符合中国国情的发展道路。党的二十届三中全会作出了关于“稳妥推进数字人民币研发和应用”的决策部署，这既是对数字人民币过去工作的肯定，也为以改革创新精神进一步推进数字人民币发展提供了根本遵循和行动指南。

一、确立数字人民币双层运营架构和相应的理论体系

数字人民币是顺应数字经济的法定货币体系建设的产物。中国研发数字人民币体系，旨在创建一种满足数字经济条件下数字形式新型人民币的发行和运行体系，这是一个全方位的改革，以此支撑中国数字经济发展，提升普惠金融水平，降低机构间互通的成本，提高货币以及支付体系运行效率。采用央行中心化管理和“中央银行-商业机构”双层运营体系，坚持并动态优化以广义账户为基础的数字形态法定货币发行、流通、支付机制。数字人民币兼具账户和价值模式，并通过数据能力建设实现全局一本账：账户模式下，可与传统银行账户体系融合互通；价值模式下可通过币串形式进行价值交换，既可在区块链上提供智能支付，也可在“无网”“无电”等离线极端场景下使用，优化了传统贸易金融业务流程，支持降本增效。

二、积极探索创新应用场景，初步构建数字人民币生态

2014 年，中国人民银行成立法定数字货币研究小组，开始对发行框架、关键技术、发行流通环境等进行专项理论研究。2016 年，成立数字货币研究所，作为推进数字人民币工作的金融基础设施单位。同年确立双层运营体系和长期演进技术路线，逐渐成为全球央行数字货币的主流标准。2022 年 1 月以

来，数字人民币 App 在各大手机应用市场上架。目前，数字人民币试点范围覆盖 17 个省（市）的 26 个地区，下一步还将继续深化。数字人民币在批发零售、餐饮文娱、教育医疗、社会治理、公共服务、乡村振兴、绿色金融等领域形成了一批可复制、可推广的应用模式，在服务国家重大战略、提升货币支付便利性和安全性、优化营商环境和数据要素市场化配置、增强人民币国际影响力等方面的作用初步显现。截至 2024 年 7 月末，数字人民币 App 累计开立个人钱包 1.8 亿个，试点地区累计交易金额 7.3 万亿元。

三、以人民为中心，持续提升服务水平

一是丰富数字人民币产品体系。在基础产品方面，按照双层运营原则，数研所和运营机构共建数字人民币 App，并构建软硬钱包体系。除扫码支付、线上支付、转账和“碰一碰”支付外，无电支付、手机 SIM 卡支付等产品也开始应用。在发挥数字化优势的同时，数字人民币体系还着力弥合“数字鸿沟”，重视无障碍适老化设计。此外，不断推动数字人民币的受理环境建设。除日常消费场景外，还着力推动地铁、公交等民生场景的便捷支付，目前青岛地铁、苏州地铁和公交、海南公交等已全面实现数字人民币硬钱包受理，“碰一碰”即可乘车，还支持无网无电应用。在 2022 年北京冬奥会以及 2023 年成都大运会和杭州亚运会上，免于下载 App 的可视卡硬钱包受到广泛欢迎，提升了境外来华人员使用数字人民币的便利度。同时，按照“不改变用户支付习惯、尽量不增加商户成本”的原则推进数字人民币与传统电子支付工具条码互通的工作，以提升使用便利度。在创新产品方面，一方面数字人民币智能合约可支持合同自动和强制执行，实现资金定向拨付和监测，已在预付资金管理、供应链金融、财政补贴等场景应用。另一方面，提供对公领域结算产品，通过多层次的结算工具叠加一栈式钱包管理和数据统计等产品，满足政府部门、核心企业和跨境电商等优化交易链路、整合上下游资源，提升管理效率和对账服务等的需求，助力其数字化转型。

二是强化央行侧基础能力支撑。按照“互联互通、分层分级、风险隔离、监管穿透、中心化管理”原则持续完善数研所运行的央行端数字人民币系统，并推进运营机构端系统配套建设，以形成对各场景应用的底层支撑，满足跨机构互联互通、规范化标准化和风险联防联控的需要，实现全局数据视图和智能化监测分析。

四、继续以改革创新精神稳妥推进数字人民币研发和应用

纵观全球，各主要经济体加快了央行数字货币研发进度，积极探索升级国内和跨境支付体系。国际清算银行于 2024 年 6 月发布的调查结果显示，在 86 家受访货币当局中，94%正在研发央行数字货币。国际组织和主要经济体的央行数字货币研发理念、路线和规则与数字人民币趋同。国际清算银行、国际货币基金组织等发布的报告也认为，数字人民币已成为全球最为领先的央行数字货币项目之一。下一步，人民银行将认真贯彻落实党的二十届三中全会精神，把握数字化发展大趋势，持续稳妥推进数字人民币研发和应用，巩固数字人民币发展的优势。

（一）完善数字人民币体制机制，服务“强大的货币”建设。当前中国经济正转向高质量发展阶段，科技创新成为发展新质生产力的核心要素，数字经济新模式与新业态层出不穷。在此背景下，央行作为法定货币发行者，有义务通过提供央行数字货币来保证公众获取央行货币的权利和渠道，这就需要对货币和央行支付体系进行数字化升级，使之成为能够适应数字经济发展的通用账户型法定数字货币。中国人民银行将建立健全数字人民币监管、运营、自律等体制机制，进一步完善顶层设计，推进制度规则体系建设，将数字人民币应用场景从零售扩展至批发，从支付扩展至包括存、贷、汇、投等在内的广义金融业务，更有效地发挥法定货币职能，提升金融资源配置效率、管理和服务能力。

（二）推进数字人民币基础能力建设，在完善现代中央银行制度中发挥服务保障作用。自上世纪 90 年代起，中国人民银行开始推进电子联行和金卡

工程，旨在减少手工操作，实现联网通用，推动全社会资金流转的电子化。而数字经济的发展需要新基建的支撑，以支持更为安全、可信、智能、便捷、高效、普惠和互通的支付需求，更有效地支撑数据要素流动，形成健康可持续的数字生态，同时支持改进提高监管技术和手段，把监管和治理贯穿创新、生产、经营、投资全过程。数字人民币在这些方面可以发挥作用。为此，一方面，在双层运营架构下，中国人民银行建设运营央行端数字人民币系统，提供交易转接和结算公共基础设施，同时引导多元主体在依法合规的前提下共同参与、公平竞争，向社会公众提供优质服务。另一方面，通过混合式系统架构和智能化的数据分析能力形成央行-参与机构全局一本账，运用监管科技手段提升统计、监测和管理能力，既要支撑央行履职，也要助力国内统一大市场的构建。

（三）以账户为基础叠加智能合约，在我国治理能力现代化转型中发挥探路者作用。党的二十届三中全会提出了“治理能力现代化”的要求，在数字经济时代，完善数字金融治理体系是治理能力现代化的重要组成部分。数字人民币可支持加载不影响货币功能的智能合约，实现智能支付，既可有效降低经济活动履约成本，提高资金发放及管理效率，赋能地方经济社会发展，优化营商环境，也可提升监管的效率和效果。在做深做细和规模化推广零售场景的基础上，金融机构之间可以用数字人民币来提升批发支付的效能，金融市场基础设施也可使用数字人民币为金融资产交易提供智能支付，便利穿透式监管。

（四）深化跨境应用和跨境基础设施建设，为金融高水平开放提供基础设施支撑。党的二十届三中全会强调要“推动金融高水平开放，稳慎扎实推进人民币国际化，发展人民币离岸市场”“建立健全跨境金融服务体系”。在数字经济背景下，要实现这些目标，离不开好用的货币和安全高效的新型金融基础设施。数字人民币采取模块化设计，可灵活对接境外央行基础设施，实现与对接的司法管辖“一通全通”，钱包开立便捷，且坚持“无损、合规、互通”原则，有助于提升不同司法管辖间的互信，在跨境应用方面具有天然的优势。前期，多边央行数字货币桥通过中央银行间合约的形式，在全球率先进入持续运营的最小可行性产品阶段，泰国央行、阿联酋央行、中国人民银行数字货币研究所、香港金管局和沙特央行作为正式成员开展真实跨境交易，观察员已扩展至 30 多家；数字人民币双边合作也取得初步进展。后续，一方面要继续在多边合作框架下完善多边央行数字货币桥等跨境支付平台，以有效解决跨境支付“成本高、效率低和透明度低”的难题。另一方面，发挥数字人民币特性，研究优化配套政策，持续探索与共建“一带一路”国家等相关友好经济体的双边合作与互联互通。此外，也要深刻认识强大的国际金融中心是金融强国的关键核心金融要素之一，将以落实内地和香港“三联通、三便利”政策为契机，深化香港数字人民币试点，巩固提升香港国际金融中心地位；以构建航运贸易数字化和相应的数字人民币支付结算体系为依托，支持上海国际金融中心建设。

（来源：时事报告 作者：中国人民银行数字货币研究所所长 穆长春）

（编辑：李彤欣）

【年会】中国法学会网络与信息法学研究会 2024 年年会暨第二届数字法治大会在云南昆明召开

原载：“网络与信息法学会”微信公众号

由中国法学会网络与信息法学研究会主办，云南大学承办，云南省大数据有限公司协办的“中国法学会网络与信息法学研究会 2024 年年会暨第二届数字法治大会”于 2024 年 9 月 21 日在云南昆明召开。本届年会的主题为“发展新质生产力的法治保障与网络法治三十年”。

大会开幕式于上午 9 时在云南海埂宾馆举行，由中国法学会副会长、网络与信息法学研究会会长，最高人民法院咨询委员会副主任姜伟主持。中国法学会党组成员、副会长张苏军，云南省法学会会长张太原，公安部十一局副局长、一级巡视员李彤，

云南大学党委书记周学斌先后致辞。

上午会议第二阶段为理事会报告环节，由中国法学会网络与信息法学研究会副会长、清华大学法学院教授申卫星主持。中国法学会网络与信息法学研究会常务副会长兼秘书长，中国社会科学院法学研究所副所长、研究员周汉华报告理事会工作。

上午会议第三阶段为主旨演讲环节，由云南大学法学院院长陈云东教授主持。

中国法学会网络与信息法学研究会副会长，中央网信办网络法治局副局长、一级巡视员尤雪云以《加强网络空间法治建设 保障网信事业高质量发展》为题作了主旨演讲，云南省大数据有限公司副总经理靳雷以《抢抓数据要素发展机遇 激发数据要素乘数效应》为题作了主旨演讲，奇安信集团副总裁、数据安全首席科学家刘前伟以《人工智能带来的新威胁及治理探索》为题作了主旨演讲，云南大学信息学院智能系统与计算创新团队带头人、副院长岳昆教授以《大数据知识工程的探索和实践》为题作了主旨演讲。

本次年会在 21 日下午设置九个分论坛，主题分别为“构建中国网络与信息法学自主知识体系”、“中国网络法治建设三十年”、“发展新质生产力的法治保障”、“人工智能高质量发展和高水平安全的法治保障”、“数字法治建设 ”、“数据安全治理与数据市场法治建设”、“平台经济创新发展促进与常态化监管”、“加强涉外网络法治建设”、“自动驾驶发展的法治保障”。分论坛详细内容见后续报道。

【年会】中国法学会网络与信息法学研究会 2024 年年会暨第二届数字法治大会分论坛成功举行

原载：“网络与信息法学会”微信公众号

“中国法学会网络与信息法学研究会 2024 年年会暨第二届数字法治大会”于 2024 年 9 月 21 日下午举办了分论坛。

分论坛一 构建中国网络与信息法学自主知识体系

分论坛一的主题为“构建中国网络与信息法学自主知识体系”，由中国法学会研究部二级巡视员王伟国主持。

学者专家们针对如何构建中国网络与信息法学自主知识体系从不同角度展开分享。海南大学法学院阎二鹏教授先以“构建自主的网络刑法学知识体系”为题介绍了构建自主网络刑法学知识体系的理论，中央党校（国家行政学院）政治和法律教研部政治建设教研室主任张效羽教授从以促进数智化新质生产力为主线推进网络与信息法学发展方面进行了探讨，中共宁夏区委党校法学教研部主任周晓军教授对习近平法治思想的原创性贡献进行了论述，强调了分论坛的指导思想和基调，贵州大学法学院杜明强副教授针对信息性人格权的法理证成进行了探讨，中南大学法学院学科办主任张新平副教授从整体上分享了对建构中国自主的网络与信息法学知识体系的路径的思考，北京师范大学法学院郭晔副教授从以“法治体系论”为范式建构中国自主数字法学知识体系进行了探讨，厦门大学法学院毛海栋助理教授重点聚焦于技术规制的概念证成和理论研究，上海对外经贸大学法学院经济法研究中心吴双副主任以将“枫桥经验”赋能数字社区治理，为完善元宇宙等数字社区的法治建设提供了思路，北京大学法学院博雅博士后王也在回归人权推定的既有路径的基础上论述了数字人权的厘定与证成。

分论坛二 中国网络法治建设三十年

分论坛二的主题为“中国网络法治建设三十年”，由中国网络空间研究院网络法治研究所所长张杨和南京社会科学院城市发展研究所所长、研究员，《南京社会科学》编辑吴海瑾主持。

北京市人民检察院党组成员、副检察长田向红对检察机关法律监督的数字化改革实践进行了报告，中国信息通信研究院互联网法律研究中心主任何波系统性地总结了中国网络法治三十年的成就与经验，广州互联网法院林北征法官基于一线法官的视角阐述了对互联网司法的实践与展望，浙江省公安厅网安总队二级技术主管王晖分享了轻罪治

理背景下“网络水军”刷量控评行为刑法规制的法教义学审视，北京警察学院法律系姚永贤副教授针对数字警务建设的运行现状及风险控制进行了总结和分析，武汉大学法学院崔凯副教授对我国数字化非羁押措施适用进行了研究探讨，苏州大学王健法学院朱嘉珺副教授以监察全覆盖为理论锚点系统性地分析了智慧监察体系的范畴界定、基本架构与运行规则。

分论坛三 发展新质生产力的法治保障

分论坛三的主题为“发展新质生产力的法治保障”，由中国法学会网络与信息法学研究会副会长，北京科技大学知识产权中心主任徐家力教授和人民法院出版社副总编辑，《数字法治》杂志副主编袁登明教授主持。

西南政法大学人工智能法学院院长陈亮教授探讨了发展新质生产力的法律困境与脱困之策，中国企业报执行副社长张有义从媒体角度对新质生产力的法治保障进行了探讨，美团数据合规总监田喜清以“新质生产力中的数据安全挑战与法律应对”为题进行了报告，科大讯飞法律大模型总工孔维骏分享了星火大模型在法律实践中的应用与探索，吉林大学法学院齐英程副教授对从排他到共享，以使用为核心的数据财产权研究进行了分享，安徽大学法学院储陈城副教授以新质生产力的法治保障为切入点对科技创新主体权利的刑法保护进行了探讨，云南大学法学院赵忠龙副教授介绍了数字经济时代程序型竞争法制度逻辑的生成，青岛大学法学院逄晓枫助理教授以盗窃罪为规制路径对侵犯数字资产行为入罪的规范审查进行了探讨，武汉大学法学院朱公欢博士生以“新质生产力驱动下平台互联互通的理论逻辑和实施进路”为题进行了分享。

分论坛四 人工智能高质量发展和高水平安全的法治保障

分论坛四的主题为“人工智能高质量发展和高水平安全的法治保障”，由中国社会科学院信息情报研究院编审李延枫主持。

北京互联网法院审判委员会专职委员孙铭溪以人工智能视阈下的人格权保护为题展开了报告，北京市中伦律师事务所合伙人陈际红律师分享了构建大模型预训练语料集的法律困境与路径思考，上海政法学院上海司法研究所徐伟教授分享了生成式人工智能部署者侵权责任研究，广东财经大学法学院姚志伟教授探讨了生成式人工智能服务提供者在私法上的法律性质，深圳大学法学院副院长宋旭光副教授以“人工智能时代的法律推理模型”为题进行了报告，中国网络空间研究院干部郭思源对生成式人工智能虚假信息危害的新发展进行了探讨，中国信通院互联网法律研究中心端晨希工程师从人工智能立法的两个层面与六个问题进行报告，广西民族大学法学院徐翕明副教授分享了“深度伪造”场景下滥用个人生物识别信息的刑法规制研究。

分论坛五 数字法治建设

分论坛五的主题为“数字法治建设”，由北京工业大学科学技术发展院副院长宋国恺教授主持。广州互联网法院邵山副院长探讨了司法裁判中的“告知－同意”规则，北京师范大学法学院薛虹教授以“网络虚拟财产与 NFT”为题进行了报告，新浪集团法务部谷海燕总经理从立法、行政监管和治理角度分析了网络暴力的治理困境，华东政法大学刑事法学院张勇教授分享了数字信用的犯罪治理，京东法律研究院执行院长李丽以“解构数据要素流通及其制度保障”为题进行了分享，阿里巴巴法律研究中心副主任顾伟博士对个人信息匿名化的实践困境与治理展望进行了探讨，上海对外经贸大学纪委综合办主任姚福生副教授从党规党纪的视角介绍了网络谣言的治理研究，北京科技大学文法学院张硕老师对政府收集个人信息的三重法治逻辑进行了探讨，西南政法大学赵自轩老师分享了网络爬取个人信息侵害企业数据权益的法律判断。

分论坛六 数据安全治理与数据市场法治建设

分论坛六的主题为“数据安全治理与数据市场法治建设”，由西北政法大学副校长张荣刚教授主持。

中山大学法学院高秦伟教授分享了公共数据

开放利用制度的民主观及法理阐释，浙江大学网络空间安全学院王春晖教授探讨了数据资源的要素价值与治理结构，西北工业大学公共政策与管理学院张敏教授以基于数据安全风险识别的数据要素流通全流程监管法律体系研究为主题进行了分享，重庆邮电大学网络空间安全与信息法学院夏燕教授以微软蓝屏事件引题分享了对数据安全的启示，四川大学法学院王竹教授分享了人工智能时代的《民法典》医疗数据治理体系，奇安信科技集团首席法律顾问马兰以“数据安全治理的挑战与思考”为题进行了报告，上海数据交易所研究院研究员许天熙分享了数据要素登记的制度功能与交易机构登记适配性研究，东南大学法学院副教授任丹丽以“企业向政府共享数据的补偿制度构建”为题进行了报告，中央财经大学法学院徐建刚副教授对侵害个人信息的损害认定进行了探讨，湘潭大学张路副研究员介绍了信用数据的规范定义及其治理应用。

分论坛七 平台经济创新发展促进与常态化监管

分论坛七由中国移动通信集团有限公司法律与监管事务部总经理于莽和《云南社会科学》副编审陈慧妮主持。

郑州大学法学院执行院长王玉辉教授以“数字经济时代平台垄断的协同治理”为题进行了报告，上海段和段律师事务所合伙人刘春泉以“滥用仅退款的电商平台治理”为题进行了报告，华东政法大学中国法治战略研究院金枫梁副研究员以“物联网技术作为动产动态质押合法化的技术路径”为题进行了报告，腾讯研究院高级研究员彭云以“常态化监管的加法和减法”为题进行了报告，浙江工商大学法学院王云霞副教授以“高质量发展背景下政府数据治理机制的转型”为题进行了报告，北京恒都律师事务所全国网络法专业委员会丁宇魁主任以“互联网平台监管责任的底线与边界”为题进行了报告，西北政法大学尉钏讲师以“私权力下网络平台经营者主体责任的重新解读”为题进行了报告，广州大学法学院狄行思讲师以“数据信托中的准信义义务”为题进行了报告，北京大成律师事务所高级合伙人邓志松《从中欧比较法角度看国内首起个人信息跨境传输法院判例》为题进行了报告。

分论坛八 加强涉外网络法治建设

分论坛八由上海师范大学人事处处长马英娟教授主持。

青岛大学法学院院长蔡颖雯教授以“上合组织数据跨境规则比较”为题进行了报告，北京大学法学院副院长、长聘副教授戴昕以“社会评分禁令与人机双标问题”为题进行了报告，中国法学会网络与信息法学研究会副秘书长、中国法学会法治研究所研究员刘金瑞以“数据跨境双轨制下个人信息出境监管豁免制度的构建”为题进行了报告，中国社会科学院国际法研究所科研处副处长、副研究员孙南翔以“网络执法领域的域外管辖机制探析”为题进行了报告，西安交通大学法学院王玥副教授以“大国战略竞争背景下的涉外网络法治建设——从近期美国保密政策动态切入”进行了报告，内蒙古大学法学院讲师李东方以“国际条约对涉人工智能犯罪的规制分析”为题进行了报告，中国移动高级法律专家杨海波以“数字经济伙伴关系协定数据跨境流动规则研究”为题进行了报告，武汉大学国际法研究所博士研究生罗旷怡以“网络空间国际法的体系化建构——从三个维度的问题意识出发”为题进行了报告，厦门大学博士研究生于丰华以“网络空间习惯国际法识别问题研究”为题进行了报告。

【年会】中国法学会网络与信息法学研究会 2024 年年会暨第二届数字法治大会圆满闭幕

原载：“网络与信息法学会”微信公众号

由中国法学会网络与信息法学研究会主办，云南大学承办，云南省大数据有限公司协办的“中国法学会网络与信息法学研究会 2024 年年会暨第二届数字法治大会”于 2024 年 9 月 22 日上午举办圆桌对话、分论坛总结和闭幕式。

第一个环节是圆桌对话，由中国法学会网络与信息法学研究会常务副秘书长、中国社会科学院法学研究所网络与信息法室副主任（主持工作）周辉主持，围绕人工智能治理问题进行交流研讨。云南

大学软件学院副教授王普明以“人工智能时代下法务数据治理问题的探索”为题，抖音集团法律研究与合作负责人丁道勤以“AIGC 数据法律问题思考”为题，蚂蚁集团隐私保护研究中心主任李海英以“大模型与个人信息合规的未来”为题，某科技公司数据合规执行总监兼 DPO 朱玲凤以“端侧大模型的应用发展与合规治理”为题，腾讯研究院高级研究员朱开鑫以“AI 版权治理”为题，同济大学法学院助理教授朱悦以“大模型是黑箱吗？”为题进行了专题发言。专题发言后，主持人和各专家围绕人工智能治理、人工智能立法、深度学习、数字化转型等问题进行了研讨。

第二个环节是分论坛总结，由中国法学会网络与信息法学研究会副秘书长、人民法院出版社丛书编辑部兼《数字法治》编辑部主任、编审兰丽专主持。北京师范大学法学院副教授郭晔，北京警察学院法律系副教授姚永贤，云南大学法学院副赵忠龙教授，深圳大学法学院副院长宋旭光副教授，中国社会科学院大学博士生谢智洁，西北工业大学公共政策与管理学院教授张敏，广州大学法学院讲师狄行思，上海师范大学人事处处长马英娟教授分别对 22 日下午的分论坛进行总结。

大会闭幕式由中国法学会网络与信息法学研究会副会长、中国人民大学法学院张新宝教授主持。中国法学会网络与信息法学研究会常务副会长兼秘书长、中国社会科学院法学研究所副所长周汉华研究员和云南大学法学院院长陈云东教授作总结发言，并对出席会议的嘉宾和承办方的工作人员表示感谢。东南大学法学院院长助理冀洋副教授代表 2025 年年会承办方发出诚挚邀请。

《数据产权论》新书发布会在京举办

原载：“商务印书馆”微信公众号

9 月 30 日，《数据产权论》新书发布会在清华大学公共管理学院举行。本次发布会由商务印书馆、清华大学中国电子数据治理工程研究院、清华大学智能法治研究院共同主办。北京大学教授、中国科学院院士梅宏，原国务院振兴东北办副主任、中国经济改革研究基金会学术委员会主任宋晓梧，中国法学会副会长、最高人民法院咨询委员会副主任、中国法学会网络与信息法学研究会会长姜伟，中国电子副总经理、中国电子数据产业集团董事长陆志鹏，商务印书馆总经理刘禹，全国人大常委会宪法与法律委员会副主任委员、清华大学法学院院长周光权，清华大学中国电子数据治理工程研究院院长、清华大学公共管理学院教授孟庆国，中国经济改革研究基金会理事长、数据要素市场化配置综合改革研究院执行院长石明磊，中国法学会网络与法学研究会副会长、中国人民大学法学院教授张新宝，《中外法学》主编、北京大学法学院教授王锡锌，中国政法大学研究生院常务副院长、中国政法大学民商经济法学院院长于飞，清华大学法学院教授、清华大学智能法治研究院院长申卫星，中国社会科学院法学研究所副研究员李广德等专家学者参加会议。会议由孟庆国教授主持。

《数据产权论》由清华大学法学院申卫星教授和中国电子信息产业集团有限公司陆志鹏副总经理合著完成，创新性地提出了数据“确权-析权-限权”的主体路径，并详细阐述了以“三分离”为中心的数据产权权利架构、以“三阶段”为脉络的数据确权路径，为构建数据产权体系提供了全面、系统、深入的视角。同时，该书重视理论与应用的结合，围绕产权运行体系的落地，提出构建“数据资源-数据元件-数据产品”三级市场，并提供了具有前瞻性和实操性的工程解决方案。

刘禹在致辞时指出，数据作为新型生产要素，已经成为价值创造的重要源泉。在构建数据产权体系的过程中，要平衡各方的利益关切、兼顾数据的开放与共享，还要坚守数据安全的底线。正是在社会各界对数据权属认定寄予强烈期待的背景下，《数据产权论》这部专著应运而生。他还总结了该书的三个显著特点：一是具有填补相关领域出版空白的意义；二是具有前沿性；三是突出了实践性。

周光权对商务印书馆与时俱进、紧跟讨论前沿

科学领域中的新问题表示敬意，对《数据产权论》的选题表达了赞许，认为该书很好梳理了“数据产权”概念的界定，较好回应了有关争论，提出了自己的立场，更对完善我国数据产权有关的法律规制提出了很多建设性意见，有助于实践中开展确权工作。最后，周光权对申卫星教授推动数据法学研究以及计算法学学科建设、人才培养等方面做出的贡献表达了感谢。

陆志鹏介绍了《数据产权论》的编制背景，表示《数据产权论》的成书和面世离不开清华大学和中国电子的精诚合作。双方深入研究分析了传统生产要素的产权发展历程和市场化配置一般规律，提出了“三三制”数据确权模型。第一个“三”是三次分离，就是把数据和信息分离、数据来源者和数据处理者分离、数据所有权和数据用益权分离；第二个“三”是三个阶段，把数据资源、数据要素、数据产品三个阶段根据三个分离赋予不同的数据权利，将数据三权分置方案纳入数据产权分立的理论框架中。

申卫星向与会嘉宾介绍了《数据产权论》一书的主要内容和行文思路。申卫星表示，数据确权、析权和限权是全书写作的基本思路。在确权方面，将“有恒产方有恒心”的理念从有体物世界贯彻到无体物的数据，通过层级化的思维方法，为解决数据确权困境提出了新的方法论。在数据析权方面，为解决信息、数据的纠缠现象，以及满足数据来源者、处理者等多元市场主体的诉求，基于“解耦”的技术概念和“人财两分”的基本理念，将信息和数据作为客体分离、数据来源者和处理者作为主体分离、所有权和用益权进行分离，实现了“三三制”确权法。在数据限权方面，本书探讨了数据合理使用、法定许可、强制许可等制度，避免因数据确权所导致的反公地悲剧现象。最后，申卫星强调，基于中国电子在四川德阳、河南郑州、浙江温州、江苏徐州等地方实践成果，本书还就数据产权制度落地中的市场运营和技术支撑方案进行了探讨，实现了理论研究与实践落地的结合。

梅宏表示，当前我国数据要素化进程已到实操阶段，数字经济新形态的有序形成和健康发展得益于三大基石：一是数据要素市场，二是数字治理体系，三是数据技术体系。《数据产权论》凝结了申教授在法学领域的前沿理论和陆总在数据要素市场化领域的实践经验，尤其是“三三制确权法”的提出极具特色，一是充分认识到了数据内部复杂的层级结构，二是关注到了数据确权涉及的隐私保护、权益界定以及收益分配的难题，三是明确提出了数据三阶段与数据三权的映射关系，对我国数据确权工作的开展具有开拓性、指导性意义。

宋晓梧指出，《数据产权论》的出版填补了我国数据要素市场化配置基础性制度的空白，具有重要参考价值和指导意义。他强调深化要素市场化配置是当前经济体制改革关键问题，数据要素作为新生产要素，其产权界定比传统要素更复杂。中国电子和清华大学的研究成果为我国数据工作做出突出贡献，所提出的“三三制”确权法和三级市场数据要素流通运行体系，不仅是一般的抽象理论的研究，还有具体的实际操作的方法和方案，体现了较高学术水平和科学价值。

姜伟从三个视角分享了《数据产权论》的学术价值和社会影响。一是认为在数据要素市场快速发展阶段，用旧制度规范新业态会束缚新质生产力的发展，本书的出版恰逢其时，具有开拓性意义。二是认为两位作者在业界都具有广泛影响，联袂著书立说，既坚持了理论联系实际，也体现了法律融合技术，还凸显了学术对接产业，建立了数据领域跨界合作的典范。三是认为本书推动了数据产权的理论创新、实践创新、制度创新，提出的数据“三三制”确权法，为建立健全数据产权制度提供了理论逻辑和实践路径。

石明磊表示，《数据产权论》在方法论上有很多值得学习和借鉴的地方，主要有四个方面。一是遵守了权利价值平衡的立场，基于“确权-析权-限权”路径开展研究；二是遵循了知识考古的立场，敢于讨论概念，敢于用知识考古学的方法来看待学问；三是遵循了精致析权的操作主义的立场，既遵循大的权利观，又符合现实生活需求；四是遵循了

面向应用的实践主义理论，以数据元件为基础，提出了一套数据确权和运营的工程路线。期待本书能够更远、更准、更加靶向地解决数据确权理论和实践难题。

张新宝首先对新书的发布表示了祝贺，认为本书在研究的方法、模式、路径等方面都具有较强的借鉴意义，提出的“三三制”数据确权方案具有较强的创新性，同时也期待这本书能够走向世界成为经典的中华学者的著作。其次结合网上购物和智能驾驶两个场景，认为个人的人格权益是需要被严格保护的，对于个人是否需要参与到数据确权以及分得相关的利益仍值得进一步深入研究。

王锡锌认为本书的出版是在数字法学、数字法治领域，对于中国提升数据产权话语权、学科建设和知识体系完善，具有非常重要的创新意义。他用四个成语表达了对本书的认识：一是继往开来，数据是数字经济、数字治理当中最重要的话题，目前需要对过往进行适当的归纳、总结、反思，而未来还有很多有待展开。二是拨云见日，从产权问题的界定入手，进一步进行析权和限权，是非常好的思路，起到了拨云见日的效果。三是强强联手，两位作者在各自领域都是学术和思想的领军者，在本书的内容中，理论与现实、理想与实践的结合也体现了强强联手的效果。四是美美与共，王锡锌对商务印书馆与两位作者的联手表示了特别的期待和祝贺。

于飞从三点对《数据产权论》给予了高度肯定。一是在数据产权方面，此书的发布表明我们正在构建一套创新的规则和理论，引领别人去学习和分享，第一个在中国自主的法学知识体系的建立上，是能够做出真实贡献的。二是《数据产权论》的两位作者背景特殊，一个纯法学的学者和一个纯技术的作者，两人共同进行法学著述的写作，是从前没有的，而这种结合又是必须的。两人创作的《数据产权论》能够真正地做到理论和实践相结合。三是《数据产权论》的核心理论“三三制”，横向的三次分离，纵向的三个阶段，在数据和权利领域里面，可以用八个字去形容“混沌已分、天下初定”，它包含了非常大的雄心要在数据和权利领域建立一个基本的秩序结构，是具有作出根本性贡献的魄力的，作出了具体性的成果。

党的二十届三中全会《决定》明确提出，“加快建立数据产权归属认定、市场交易、权益分配、利益保护制度”。在此背景下，数据产权体系设计已成为数据要素市场化配置改革中亟待破解的关键命题。合理有效构建数据产权体系，对数据要素形成过程中各参与方的“权、责、利”做出清晰界定，将对数据市场的高质量发展产生重要影响。《数据产权论》的出版，对于推动我国数据产权制度的建立和完善、促进数据资源的合理开发和利用、保护公民和企业的合法权益将发挥重要指导作用。

（技术编辑：王藜焯、敖紫辰）

研究动态

基础理论

1. 从部门立法到领域立法：数字时代国家立法新趋势（周佑勇）

来源：《现代法学》2024 年第 5 期

数字时代的社会风险问题逐渐呈现出领域性、复合性、交叉性等特征，而传统的法治资源供给路径则因循部门立法模式，容易造成法律规范的“碎片化”与部门壁垒，导致单一的部门法规范与复合性社会实践问题之间出现鸿沟。基于国家治理现代化的需要，领域立法已成为新兴交叉问题的重要法律规制范式，它通过统筹考虑各种法治资源的属性、功能及其协调关系，可以促进不同学科知识实现跨领域的交叉融合，为领域性问题提供立体化的综合性解决方案。数字时代领域立法的发展路径应以领域性的重点风险问题为立法导向，在横向上要强化传统部门立法之间的协同关系，整合各个部门法的知识体系；在纵向上则需建立法学与其他人文社会科学、自然科学等学科之间的联结关系，促进形成领域问题的跨界融合治理方案。

2. 数字立法基本范畴的分层逻辑与统合方式（任颖）

来源：《政治与法律》2024 年第 9 期

数字立法是新兴领域立法的重要方面，基本范畴是数字立法的逻辑起点。数字立法基本范畴从目的论、对象论、方法论三个方面，为数字立法实践提供理论支持。在目的范畴方面，数字立法基本范畴的逻辑同构以“人本回归”为核心，以数字身份、数字契约、数字人格三元结构为基础，从不同单行立法之间的逻辑关联出发，为数据风险、信息风险、算法风险治理制度的衔接奠定理论基础。在对象范畴方面，数字立法基本范畴的分层逻辑，以数据、信息、算法三重社会关系调整为核心，形成数字立法基本范畴的分异结构。这一分异结构反映不同立法范畴之间的逻辑差异，奠定数据、信息、算法区分立法的理论基础。数字立法方法范畴的逻辑发展，从立法体系与范畴体系的内在对应关系出发，形成数字时代的赋能授权、私权规制、权利构造逻辑，推进数字公权力、平台私权力、社会私权利配置的结构性平衡。数字立法的健全和完善，以数字立法

基本范畴的分异结构与逻辑同构为脉络，以数字单行法向数字基本法的进阶为支撑，分阶段、分步骤推动数字法律制度的多层次协调，形成数字行为法、责任法、程序法的协调发展格局，推动数据安全风险评估、个人信息保护影响评估、算法安全评估程序等规范的衔接，促进数字私益、数字公益、数字众益等价值衡量机制建设，实现数据安全审查、信息合规审计、算法合规审查等法律制度协同。

3. 论技术范式转移下元宇宙的法律治理（马永强）

来源：《中国法学》2024 年第 5 期

元宇宙实践中从 Web2 到 Web3 的技术范式转移，其表象是“中心化”与“去中心化”的技术标准之争，本质上则揭示了元宇宙实践中围绕虚拟世界的治理权力展开的多方博弈。深度数字化时代虚拟空间的发展方向集中体现为互联网巨头主导的元宇宙实践与去中心化自治组织主导的元宇宙实践共存共生，二者均可能在不同维度上侵害个体的数字权利，并给现实世界中主权国家的治理权力带来挑战。应准确评估不同形态的元宇宙虚拟空间的现实风险，并区分不同情境有针对性地制定法律规则，系统构建元宇宙的法律治理路径。公权力应强化对科技巨头的反垄断和对去中心化领域的监管，贯彻中心化与去中心化动态平衡的治理理念，建构基于元宇宙底层技术和应用场景的多元共治的治理体系，探索事前介入、合法性监管以及“法律代码化”的治理方式，明确刑法的理性介入为元宇宙实践划定的治理底线。

4. “数字枫桥”的法治原理、模式与机制（杨力）

来源：《中国法学》2024 年第 5 期

数字化拓展了对社会改造的可能性，已对纠纷解决产生深刻影响，其中既有纠纷的数字化治理，也有数字化带来的挑战。作为纠纷解决的新形态，“数字枫桥”聚焦的不是简单发挥数字本身的禀赋，而是把纠纷解决的要素转化进入社会性、法律性的相互关系，是对纠纷解决的结构、资源和规则的数字化重组，重新界定了“枫桥经验”的法治内涵、定位和功能。在此基础上，引入行为动力理论可以进一步解释“数字枫桥”何以能成为推动纠纷解决范式从“硬性干预”到“柔性干预”转型的动力机制，塑造新型的法治模式。“数字枫桥”需要推动法治机制创新，树立多元规则择优的标准，构建嵌入规则的平台体系以及建立稳定预期的信任规则。

5. 数字脆弱性：重新思考数字时代的力量失衡（Michelle LIU）

来源：European Review of Private Law, Vol.32, Issue 5 (2024)

考虑到市场上的权力不平衡，欧盟法律对主体的弱势地位及其原因做出了一些假设，例如消费者和数据主体。然而，权力不平衡已经由于数字化而显著加剧。于是就引出了一个问题，即欧盟法律是否充分有助于纠正数字环境中的力量不平衡，如果不足以纠正，欧盟法律应该采取什么方向来应对数字时代的挑战。首先，本文阐述了欧盟法律关于主体弱势地位的假设及其原因。其次，本文对这些假设进行仔细审查，以调查它们是否恰当地反映了力量失衡。第三，某些假设在当前的数字现实中可能不再成立，因此讨论了欧盟法律对力量不平衡的分歧。第四，文章提出了欧盟法律应考虑的因素，以适当地捕捉数字时代的力量失衡。在此基础上，本文提出了解决数字增强的力量失衡的切实可行的解决方案。

个人信息保护

1. 个人信息保护检察公益诉讼的路径优化：以多元协同理念为核心（陶加培）

来源：《华东政法大学学报》2024 年第 5 期

个人信息保护检察公益诉讼是数字时代背景下个人信息国家保护主义的有效司法路径。当前，我国个人信息保护检察公益诉讼相关法律规定内

容相对原则且分散，使制度整体面临理念、规范与实践的多维治理困境，难以回应数字时代个人信息公益保护的治理需求。推动个人信息保护检察公益诉讼的路径优化，确有必要建构以多元协同理念为核心的治理体系，实现多元治理主体、多维治理目的和多类治理机制的协同共治。以“检察公益诉讼法”立法为契机，强化个人信息公益保护的规范供给，既要建构内部框架秩序，弥补诉权主体正当、公私益判断标准、程序处理机制、诉讼责任承担等方面的疏漏，又要搭建外部治理机制，引入积极能动的检察理念和诉源治理机制，完善公益诉讼赔偿金管理使用机制。

2. 个人信息诉讼前置程序的模式选择与解释路径（苏和生）

来源：《华东政法大学学报》2024 年第 5 期

《个人信息保护法》第 50 条是否确立了强制性诉讼前置程序，理论界与实务界对此争议颇多。与“行政机关主导强制适用”“信息主体主导选择适用”等模式相比，“信息处理者主导强制适用”模式遵循了个人信息保护请求权特殊的构造机理，更契合《个人信息保护法》的立法宗旨与法条文义。相较于诉讼程序，个人信息诉讼前置程序更具便捷性、效益性和自治性，能助益于个人信息纠纷的有效预防与实质性化解，但作为和解型前置程序，其在程序构造、程序主导者配置方面的弊端不容忽视。实现增量保障功能是前置程序的正当性基础，应检视前置程序能否促进实体权利行使、保障程序权利，并增强权利救济效果。鉴于前置程序的普及适用极易对当事人诉权造成系统性冲击，宜通过解释论消解当前困境，即引入三阶审查框架(请求权基础→便捷性标准→履行程序的正当性)划定前置程序的运行空间，妥善限缩其适用范围。

3. 侵犯公民个人信息罪保护法益的厘清（敬力嘉）

来源：《现代法学》2024 年第 5 期

由于缺乏对个人信息与个人数据关系的正确认识，所以侵犯公民个人信息罪既有法益观的权属配置视角存在欠缺，在具体适用中面临诸多障碍。在个人数据流通的现实场景中，应承认本罪的行为对象包含承载个人信息的个人数据。基于本罪保护法益的确立依据，即行为对象的社会属性，行为内容的场景属性与危害后果的多元属性，应将本罪的保护法益确立为法定主体的信息专有权，其支配主体、法益内容与法益属性均应遵循场景化判断标准。以此为指导，可明确本罪行为不法的动态判断机制，厘清侵犯公民个人信息的行政不法与本罪刑事不法，以及本罪与关联犯罪的区分标准，将个人数据关联主体权益妥善纳入本罪的保护范围。

4. 侵犯个人信息行为的刑法全流程规制模式研究（童云峰）

来源：《现代法学》2024 年第 5 期

在个人信息行为规制方面，我国前置法与刑法之间存在明显差异，前置法通过处理规则的设计实现了全流程规制，而刑法只能对部分不法处理行为进行惩治。此种规范格局导致法律难以衔接并形成刑法保护的盲区，不利于全面保护个人信息权益。对此，应提倡个人信息的刑法全流程规制模式，通过间接罪名适用法和法益量刑评价法对不同类型处理行为进行合理规制。通过理论维度和规范维度的证成，可以验证全流程规制模式具有可操作性。应当适用刑法合理规制非法收集行为和非法存储行为，保障前期阶段信息处理安全；适用刑法精准规制非法加工行为、非法使用行为和非法流转行为，保障中期阶段信息处理安全；运用刑法适度规制非法披露行为和非法删除行为，保障后期阶段信息处理安全。

5. 民事公益诉讼在个人信息保护中的实现机理（张振宇）

来源：《政法论坛》2024 年第 5 期

数字经济时代，个人信息兼具私益与公益的双重性质，因而需要在私法与公法有效互动的前提下才能得到保护，而民事公益诉讼制度与个人信息保

护的特殊需求相符合，对民事公益诉讼于个人信息保护中的实现机理展开探究具有重要意义。当前，个人信息保护民事公益诉讼制度的运行主要体现在法律机理、实践机理与技术机理三方面。从理论和实践出发，该制度运行仍面临着诉讼主体不明确、救济客体难认定、制度保障争议大和公益诉讼衔接弱的现实挑战。为此，应当明确诉讼主体的权利义务，制定个人信息权益损害认定规则，完善侵权人的责任承担方式，协同个人信息保护诉讼关系，以厘清民事公益诉讼在个人信息保护中的实现机理，维护社会公众的信息权益。

6. 公开个人信息的刑法保护：理念、进路与边界（郑泽星）

来源：《政法论坛》2024 年第 5 期

用刑事手段规制非法处理公开个人信息的行为应当坚持必要性和谦抑性理念。确定公开个人信息刑法保护边界的应然进路是在公开个人信息类型化的基础上实现前置法规定与刑事法规范之间的融贯。以公开意愿为依据可以将公开个人信息区分为主动公开信息、被动公开信息以及非法公开信息。前置法的“合理处理”规则是义务性规范，违反“合理处理”规则无涉侵犯公民个人信息罪保护法益，可能导致民事责任或者行政责任；“明确拒绝”规则和“重大影响”规则是禁止性规范：主动公开的个人信息，权利人“明确拒绝”的，其恢复行使个人信息自决权；被动公开的个人信息，权利人“明确拒绝”的，其保留行使个人信息自决权。对上述信息的处理均可因侵害个人信息自决权法益而构成侵犯公民个人信息罪。处理公开个人信息违反前置法“重大影响”规则，使公民人身、财产安全受到重大损害或者具有重大损害风险的，仍可因侵犯公民信息安全法益而构成侵犯公民个人信息罪。

7. “被遗忘权可被删除权替代说”之质疑（邹立军）

来源：《政法论坛》2024 年第 5 期

被遗忘权的具体构成不同于删除权。被遗忘权的实质在于遗忘，而不在于删除。被遗忘权是由遗忘权与删除权融合而成的在线权利，对个人信息的一种控制保留的权利。遗忘权是使个人信息权利主体免受过时的、不当的、不相关的负面信息困扰或伤害而设立的权利，目的是维护人的尊严和自由。程序性权利的删除权是个人信息权利主体为了实现遗忘权，向个人信息处理者请求删除，经其审查没有例外保留个人信息的必要性，依法采取删除等技术措施，区分作为被遗忘权的义务主体，以决定是否具有通知相关个人信息处理者的义务，从而达到防止个人信息扩散的目的。被遗忘权不能被删除权替代，我国应当考虑设立被遗忘权。

8. 论政府部门涉税信息共享中的个人信息保护（杨同宇）

来源：《中国法律评论》2024 年第 5 期

政府部门涉税信息共享应遵循比例原则，其正当性审查的首要基准在于是否遵循目的正当性，即税收征管的共享目的是否明确、合理、限定；其后在适当性层面考察共享行为同应税事实认定之间是否存在实质关联性；在必要性层面考察共享行为是否对纳税人合法权益影响最小；在均衡性层面考察共享目的与对纳税人合法权益的影响是否合比例。从主体权利观之，纳税人基于纳税人角色和个人信息主体角色分别享有纳税人权利和个人信息主体权利，厘清两类权利规范的适用逻辑有助于最大化实现主体权利。就机制完善而言，在立法层面，《税收征收管理法》应对政府部门涉税信息共享个人信息保护基本规范类型予以补足；在实施层面，应充分发挥税收征管与个人信息保护二元机制的合力作用，推进统一平台建设。

9. 数据跨境双轨制下个人信息出境监管豁免制度的适用与完善（刘金瑞）

来源：《财经法学》2024 年第 5 期

数据跨境新规确立了个人信息出境监管豁免制度，既豁免了申报数据出境安全评估，也豁免了

订立个人信息出境标准合同、通过个人信息保护认证。但从我国数据跨境管理双轨制体系来看，这些豁免规则在理解适用上仍存在一系列困惑：符合场景豁免的个人信息是否必然豁免安全评估，一定数量个人信息为何可以豁免同等保护要求出境，过境个人信息豁免、负面清单外豁免的合理限度何在，实践需要与安全关切双重压力下应如何完善豁免。破解这些困惑，就应该明确特定豁免只是豁免保护个人权益的监管机制，厘清个人信息与重要数据关系以明确豁免边界，系统把握过境个人信息豁免和负面清单外豁免，增强数据跨境制度协同性以缓解豁免规则压力。

10. 个人信息匿名化制度的反思与改进（夏庆锋）

来源：《财经法学》2024 年第 5 期

我国《个人信息保护法》第 73 条规定匿名化是指个人信息经过处理无法识别特定自然人且不能复原的过程，并在第 4 条对匿名化信息进行豁免保护，采用静态匿名化的方法平衡个人信息保护与个人信息利用。但是，伴随社会信息化以及网络技术的快速发展，匿名化信息与非匿名化个人信息的界限趋于模糊，强大的经济激励使去匿名化具有针对性，导致重新识别的匿名化信息对信息主体产生侵害风险甚至现实损害。虽然已有网络服务商承诺、合同义务约定与立法直接禁止等措施对去匿名化进行制约，但未能实现较好的规制效果，应在现有匿名化制度中加入更为灵活的动态匿名化方法。当匿名化信息的使用可能产生损害或是由于语境的变化使匿名化信息具有识别性时需进行更为严格的再匿名化处理，否则不真正匿名化信息仍需受到法律保护。

11. 数据保护局的独立性和“间接”访问——在比利时、法国和德国是虚幻的？（Diana Dimitrova & Paul De Hert）

来源：Maastricht Journal of European and Comparative Law, Vol.31, Issue 1 (2024)

第 2016/680 号指令规定了行使个人数据访问权的两种程序：直接程序（即直接针对执法机构）和“间接”程序，其中负责的数据保护局对拒绝直接访问的执法机构行使数据主体的访问权，包括对请求访问的个人数据的数据处理进行合法性检查。最近对人权联盟的判决将数据保护局在该程序框架内的权力问题视为数据保护局的独立性问题。现有文献观察到，比利时、法国和德国这三个成员国的执行法律在执行“间接”访问权时，严重限制了数据保护局的权力，例如进行合法性检查并将检查结果通知个人。本文认为，这些国家限制构成了对欧盟数据保护法中数据保护局独立性要求的不合理干涉，包括欧盟基本权利宪章第 8（3）条。

数据确权与流通

1. 刑事诉讼数据处理的全流程监管（郑曦）

来源：《中国法学》2024 年第 5 期

数字时代的刑事诉讼越来越倚重于数据处理，而数据处理涉及重大法益，应对其进行全流程监管。为实现此种监管，应以数据处理活动为监管内容、以检察机关为监管主体、以具有公权力属性的数据处理者为监管对象，勾勒出刑事诉讼数据处理全流程监管的基本架构。刑事诉讼数据处理全流程监管应以权力行使与权利保障平衡为价值取向、以数据流动与数据安全兼顾为监管目标，采用“面”“线”“点”相结合的监管方式，为数据监管工作提供指引。在具体实施层面，应围绕数据的收集、使用与加工、存储与传输、删除与销毁四个数据处理的核心阶段展开监管，以保护公民权利，并保障数据的安全和有序流动。

2. 财产事实支配的宪法定位及其在数据财产领域的运用（杜牧真）

来源：《中国法学》2024 年第 5 期

财产事实支配作为一种自由，是宪法和法律形成的财产权所保护的对象而非财产权本身。对于作为有别于权利的财产事实支配自由，宪法和法律无需加以创设，而只能予以确认并保护。为防止财产

事实支配可能受到过度限制或不当干涉，对于财产权人与非财产权人的财产事实支配自由，我国宪法均以“法无限制即可为”的方式予以确认并保护。宪法对于财产事实支配的确认与保护，为国家设立了财产事实支配的保护义务，这包括国家消极保护义务与国家积极保护义务两方面。国家消极保护义务意味着，立法者不得以“法无授权不可为”的方式限制事实支配自由；国家积极保护义务意味着，立法者应具体形成能够保护公民对其财产的事实支配不受其他主体干涉的权利，从而使事实支配的国家积极保护义务在私权领域得以充分实现。基于财产事实支配的宪法定位可知，反对数据财产权利化的观点不能成立。

3. 个人数据交易的私法制度构造研究（夏庆锋）

来源：《中国法学》2024 年第 5 期

个人数据交易是新兴技术服务于个人的必要活动之一，只有进行个人数据的收集与分析，网络服务商等数据处理者才能提供更加符合个人需求的产品与服务。然而实践中由于当事人缔约地位存在差距等原因，个人数据失控与公正价值丧失等问题时有发生，而现行私法无法有效规制。前述问题的解决需以构造个人数据交易的私法制度为基础，具体包括主客体明确、权利配置与规则设置等。个人数据交易的主体应区分初级交易和次级交易确认，初级交易的主体包括个人与数据处理者，次级交易则发生于不同数据处理者之间；就客体而言，应明确的是，个人信息包含于个人数据，两者并非等同关系；在权利配置中，应确认个人享有数据交易全过程知情权、有限的不受自动化决策支配权等基于个人信息保护法的各项权利，数据处理者享有三权分置的数据产权以及与个人共同享有收益分配权；而在规则设置上，应协调与完善相关法律规则，包括合同法规则平衡交易主体的当事人地位、个人信息保护法规则保护个人知情同意权利与物权法规则保护处理者数据产品权益等。

1. 人工智能立法中的规制结构设计（宋华琳）

来源：《华东政法大学学报》2024 年第 5 期

人工智能统一立法应引入包容审慎监管理念，为人工智能相关法律、政策、规范的出台设置“缓和期”，可通过引入监管沙盒制度，在沙盒试点中提供规制环境。应引入风险分级分类规制理念，对人工智能应用实施分级、分类、差异化监管。立法应建构人工智能合作治理体系，让地方人民政府编制人工智能规划，以智能服务券等措施提供激励；立法可设计统分式齐抓共管的部门职责分工模式，规定人工智能监督管理协调机制；在“受规制的自我规制”制度下，人工智能开发者、提供者应采取风险管理措施，披露特定信息，制定自我规制规则，夯实组织化保障义务；还应探索第三方治理、专家咨询的制度空间。立法应建构人工智能规制的多元规范体系，明确国家标准、行业标准的功能，拓展团体标准的空间，并注重发挥伦理规范的作用。

2. 人工智能立法体系化的理论证成与路径选择（陈亮、张翔）

来源：《华东政法大学学报》2024 年第 5 期

人工智能立法体系化是全球人工智能法治的大势所趋，也是协同治理的重要抓手、科学立法的应有之义和法学知识的素材支撑。然而，当前人工智能立法研究存在“概念不清”“定性不准”“理念不彰”“范畴不明”“脉络不畅”五大问题，阻滞了立法体系化进程。应当从“人工智能的应然法律概念”“人工智能法律规范的属性”“人工智能立法的理念欲求”三个层次设置“滤网”，在区分“狭义的人工智能立法”和“广义的人工智能领域立法”的基础上锚定人工智能立法范畴。针对当前人工智能立法“碎片化”的现象，应当坚持以“事物本质”理念检视问题，在法律体系化方法中嵌入“系统—控制论”原理来规整领域立法素材。在此基础上，应当在“法律”层级适时制定一部兼具框架性和包容性的“人工智能法”，以“发展负责任的人工智能”为融贯立法体系的价值基础，以“平衡公平与效率”和“平衡

安全与创新”为两大基本原则。此外，以人工智能全生命周期的“研发—生产—服务—使用”节点为横轴，以“具体风险控制”和“抽象权利保护”两种控制模式为纵轴，可以纵横交错编织出八个具有规范生成功能的法律关系定型“区间”，由此形成构筑人工智能立法制度谱系的基本线索。

3. 无过错责任与人工智能发展——基于法律经济分析的一个观点（戴昕）

来源：《华东政法大学学报》2024 年第 5 期

如何制定人工智能致害的侵权责任规则，是人工智能立法领域的一个困难议题。由于黑箱系统的作用机制难以解释，以及致害过程有多方参与，人工智能致害侵权如适用过失责任，将产生较高制度成本。适用无过错责任不仅制度成本更低、救济效果更好，而且结合法律经济分析有关责任规则影响注意水平和行为水平的原理，可知其未必会导致对人工智能创新活动的过度抑制。同时，尽管基于行政监管的风险规制是应对人工智能致害风险的最主要制度形态，但侵权赔偿责任，特别是无过错责任的设置，将有助于维护社会对人工智能产业及人工智能监管体制的信任。

4. 自动驾驶汽车交通肇事的刑法归责（魏超）

来源：《环球法律评论》2024 年第 5 期

自动驾驶汽车的事故原因包括存在制造缺陷与存在设计缺陷两种，在因后者造成的事故中，制造商违反了注意义务，创设出了法不容许的风险，具有刑事违法性。自动驾驶汽车的使用者及制造商与法益损害均存在因果关系，基于信赖原则，使用者对“违反交通法规”不具有预见可能性，无须承担刑事责任。成立过失犯不要求行为人认识到具体的因果流程与致害行为，故只要制造商违反注意义务，创设出法不容许的风险，便对法益损害具有预见可能性，算法黑箱不能阻却其刑事责任。算法歧视有违法治国家平等保护之基本理念，在并未完全避免的情况下，原则上不应允许自动驾驶汽车上路。

5. 论我国人工智能立法的定位（周汉华）

来源：《现代法学》2024 年第 5 期

人工智能在我国已经形成信息内容管理与科技、产业发展两种不同立法定位。用信息内容管理定位人工智能，相当于将新质生产力纳入上层建筑管理，难免产生各种错配现象。为了体现人工智能法非对称性特点，需要将人工智能作为前沿科技和新质生产力来定位，在明确安全与发展基本原则的基础上，通过不同部门法的立改废释实现法治范式变革。既要清理、废止不利于人工智能发展的规定与做法，又要确立有利于推动人工智能安全与发展的观念、规范与制度。我国人工智能立法需要保持灵活性，小步快跑，避免“一刀切”立法造成难以挽回的负面影响。

6. 基础模型训练的著作权问题：理论澄清与规则适用（陶乾）

来源：《政法论坛》2024 年第 5 期

人工智能基础模型训练使用作品引发的侵权争议不断发生，对此需要从著作权法的基本法理出发，在解释学视角下进行行为定性和分类分级施加合规义务。从行为主体上，区分数据集创建者和模型开发者；从行为对象上，区分作为内容的作品与作为载体的数据；从行为样态上，将模型训练流程解构为数据准备、数据投喂与机器学习三个阶段。在第一阶段，数据集创建者在使用自有数据、购买第三方数据和抓取公开数据三种情形下对著作权侵权内容的注意义务程度依次减轻。数据集创建者复制作品是否侵权，需区分对待通用数据集和专门数据集，前者在公共利益原则下能够豁免侵权责任，后者因其整体价值与作品价值的重合性，则难辞其咎；在第二阶段，基础模型开发者通过交易行为获得数据集产品时，对数据内容的著作权合规义务有限。其将数据集投喂给模型时，对数据样本中的作品的复制是一种过程性复制，不构成侵权；在第三阶段，机器学习的对象是数据，核心目的是获取表达符号之间的分布规律，未发生对作品的呈现式或演绎式使用。鉴于著作权法意义上的作品使用指向

的是“表达性使用”，故这种“非表达性使用”不落入著作权人专有权利的控制范围。

7. 机器学习的著作权侵权判定：超越非表达性使用理论（涂藤）

来源：《政治与法律》2024 年第 10 期

针对人工智能机器学习的著作权侵权判定难题，近期引人注目的非表达性使用理论根据“表达性机器学习”和“非表达性机器学习”的类型化方法划分侵权责任，并提倡禁止人工智能模仿特定作者的个人创作风格。然而，复制权的目的解释、历史解释和判例分析表明，非表达性使用理论未能走出长久以来“实施复制即侵权”的理论误区，面临逻辑、法理和现实层面的三重困境。对此，应当对非表达性使用理论进行扬弃，重构机器学习的著作权侵权判定标准，以公众接触原作品表达的高度盖然性取代“实施复制即侵权”的形式主义理念。

8. 赋能型人工智能治理的理念确立与机制构建（张吉豫）

来源：《中国法学》2024 年第 5 期

人工智能治理已成为国家和社会治理的前沿问题和重要领域。然而，当前在人工智能科技创新、风险防控、企业自治、政府监管、社会监督、国际协作等方面都亟需加强能力建设，必须把提升人工智能安全可信发展的能力作为人工智能治理的第一要务，构建“赋能型人工智能治理”的理念和机制。以此为目标，应坚持以人为本、发展导向的赋能型人工智能治理核心理念，以及从中发展出的智能向善、包容审慎、敏捷治理、可持续发展等基本理念。应建设以法治为核心的赋能型人工智能治理机制以及法治统领下的各项具体机制，如完善法律治理与技术治理相统合的机制，建立多元主体沟通协作的共治机制，构建与人工智能发展相适配的“避风港”机制，建立敏捷互动、激励向善发展的动态监管机制，建设人工智能安全保险等社会保障机制。

9. 论人工智能立法的基本路径（林洹民）

来源：《中国法学》2024 年第 5 期

采用何种路径规范人工智能活动，是人工智能立法的核心问题。风险管理进路存在风险评估与分类困难、放任损害发生等问题，并非人工智能立法的当然选择。与以往科技活动不同，人工智能活动既属于专精科技活动，又具有赋能科技活动属性。以人工智能活动为规范对象的人工智能法不应以单一理论为指导，而应遵从科技法与应用法双重定位。科技法定位下的《人工智能法》应尊重科技自主，将科技伦理内化于人工智能研发活动中，同时打破制度壁垒，设计促进型规则，助力人工智能科技的发展。应用法定位下的《人工智能法》则应关注科技赋能场景导致的功能异化现象，一方面借助抽象的权利义务工具，尤其是通过规定新型权利，构建弹性的规范框架，回应不同应用场景中的价值序列差异；另一方面应推行实验主义治理，通过监管沙箱、授权性立法等设计，动态调整监管策略，满足人工智能赋能应用活动的灵活治理需求。

10. AI 生成声音侵害声音权益的法律认定——以殷某某诉北京某智能科技公司等人格权侵权案为例（北京互联网法院课题组）

来源：《法律适用》2024 年第 9 期

自然人声音具有独特性、唯一性、稳定性，可以标表自然人身份，既体现人格尊严，亦带有明显的财产属性，未经许可使用他人声音构成侵权。声音是否具备可识别性以及 AI 生成声音是否具备可识别性，贯穿 AI 生成声音侵害人格权认定全链条，前者既关乎他人未经许可使用的行为是否构成侵权，又决定了有无必要进行后者的判断；后者关乎自然人声音能否及于 AI 生成声音以及未经许可使用该 AI 生成声音是否构成侵权，可以从主观标准、客观标准、使用方式三方面综合判定，主观标准应以一般社会公众或一定范围内的公众能否识别来判断，客观标准可以从声纹辨认、声纹确认、声音的音色、语调等方面综合判断。损害后果按照侵权情节、同类市场产品价值等因素综合考量。

11. 人工智能赋能社会治理的法治路径（赵豪）

来源：《法律适用》2024 年第 9 期

利用人工智能为社会治理赋能，已经成为智能时代治理转型的必然方向。这一治理范式从公共部门角色转型与社会共治两方面提升了国家治理水平。我国为实现国家治理体系和治理能力现代化，亦需借助人工智能技术赋能自身，从而在社会治理方面取得更大成就。但社会治理智能化的变革隐藏着权力运行失衡、体系移植不匹配以及信息安全受威胁等隐患，同时在实践中还需要在政务数据共享、公共部门人员技术适配性以及相对人接受程度等方面持续探索。为此，应当基于系统化视角，从基础、起点、过程和回顾四个层面对人工智能赋能社会治理的数据、智能治理工具的参与边界、智能化社会治理中的风险控制及其法治评估等问题进行制度设计，从而构建具有开放性和发展性的智能治理法治框架。

12. 由 ChatGPT 窥探智能时代我国著作权法坚守与变革（黄细江）

来源：《知识产权》2024 年第 8 期

“以人为本”是人工智能的根本理念，我国著作权法的作者权模式一开始就注定恪守作者中心主义。人工智能生成内容不能脱离主客体不可置换的逻辑基础，当其通过“图灵测试”、符合独创性要求时，考虑法的安定性、伦理性及帕累托最优，将其作为作品保护成为最优选择，使用者是作者。它仍以现有作品法定类型为依据，权利内容、权利保护期限不变，标记是获得诉讼保护的前提。而人工智能数据输入和机器学习尽管会使用受保护的作品及其片段，但因这种使用是非表达性使用、非竞争性使用，能够产生新知并促进人类整体发展，属于合理使用。未来我国著作权法应增加“文本与数据挖掘”合理使用特别条款。

13. 人工智能基础模型安全风险的平台治理（周辉）

来源：《财经法学》2024 年第 5 期

人工智能基础模型的安全治理是人工智能法治化发展面临的重要命题。人工智能基础模型平台作为安全治理的主体，其发现、评估和缓解人工智能系统潜在风险的能力至关重要，具有调整和优化自身模型的作用。国内外人工智能基础模型平台积极布局安全风险治理，但仍然面临治理架构缺乏权威性和代表性、伦理规范过于抽象、测试算力不足、风险评估困难、平台存在利己偏好等挑战。有必要立足于中国人工智能基础模型平台安全治理的实际，完善压力驱动、动力保障、能力强化等机制，更好发挥人工智能基础模型平台对安全治理的特有优势和能动作用，支撑人工智能技术及其应用健康有序发展。

14. 引导人工智能系统对工作场所的影响：从劳工角度看欧盟人工智能法案的优势和漏洞（Chiara Cristofolini）

来源：Italian Labour Law e-Journal, Vol.17, Issue 1 (2024)

人工智能（AI）在工作场所的快速整合带来了机遇和风险。它可以提高生产力和工作条件，但如果应用不当或使用不透明，可能会加剧现有的脆弱性。欧盟人工智能领域的发展推动了立法的努力，最引人注目的是期待已久的《人工智能法案》。本文旨在研究此类法规对人工智能系统在工作领域使用的影响，并对其法律框架进行首次评估。本文认为，虽然欧盟人工智能法案改进了以前的草案，但含糊不清和漏洞仍然存在。然而，它也指出该规定只提供了一个最低限度的共同框架，为更有利的规定或集体协议留下了空间。在此背景下，本文强调了社会合作伙伴在制定规范在工作场所使用人工智能的场景化法规方面的关键作用，并在结论中确认，只有多方利益相关者的协同作用才能跟上人工智能等快速发展的技术的步伐。

平台治理

1. 数字平台治理的“两面性”及刑法介入机制（房慧颖）

来源：《华东政法大学学报》2024 年第 5 期

提升数字平台的常态化监管水平，推动数字平台规范健康发展，是提高数字经济背景下经济风险防控能力的有机组成，也是提升我国治理能力现代化水平的时代课题。刑法在介入数字平台治理时面临诸多难题：在治理主体方面，呈现出“重监管，轻内控”的特征，无法有效激发数字平台保障自身有序发展的内生动力；在治理目标方面，呈现出“重规制，轻发展”的特征，忽视了制度规范的过度束缚对数字经济和科技发展的负面作用；在治理规范方面，呈现出“重制度，轻技术”的特征，信息不对称和技术壁垒等因素使传统监管模式陷入力所不逮之困境。为此，应根据技术发展新实践，确定技术治理新机制。构建二元治理机制，形成“自治”与“他治”的双向互动，促进外部监管与平台内控的有机融合；构建三阶治理机制，妥当把握刑法介入数字平台监管的时机和限度，平衡规制与发展之间的关系；构建合作治理机制，发挥利用技术手段监管技术风险的优势，克服传统治理方式的缺陷，实现对数字平台风险的实时、动态、有效治理。革新数字平台刑法治理体制工具，创新数字平台刑法治理实践进路，有利于保障数字平台平稳运行，促进数字经济行稳致远。

2. 算法推荐平台版权注意义务：法理解构与规范路径（初萌）

来源：《知识产权》2024 年第 8 期

以危险控制力和损害原因力作为区分依据，网络平台版权注意义务包括消极的注意义务和积极的注意义务，体现为三种具体的类型：一是基于侵权信息明显程度的消极注意义务，二是基于平台运营方式所致较大侵权风险的消极注意义务，三是基于损害原因力的积极注意义务。算法推荐技术的运用虽未显著提升平台危险控制力，但基于拟态环境的塑造改变了平台与传播行为之间的损害原因力，故应当相应提升注意义务。内容过滤仅是算法推荐服务提供者注意义务的一个组成部分，且适用范围应有所限制；算法推荐服务提供者的注意义务应当从推送信息的选择、算法运作机理的设置和外部规则的引入三个维度来建构，从基于内容的注意义务转向基于技术的注意义务。

3. 网络平台行为规制中的基本权利私人间效力论之否定（刘爱茹）

来源：《财经法学》2024 年第 5 期

对于我国应否接受基本权利私人间效力论，并将其运用于近年来热议的网络平台行为规制当中，有必要从实践角度提供参考。基本权利私人间效力论之实践，主要包括立法和司法机关在基本权利保护的指引下进行民事立法和司法，以及有权机关对立法和司法机关基本权利保护义务履行之审查。基本权利私人间效力论本欲全面实现基本权利的价值、完善部门法的实施，并更有效地保护基本权利。但相关实践不仅无法实现其目标，反而导致基本权利价值贬损、部门法的独立性和法的安定性受到破坏，并不利于基本权利的保护。通过实践考察及反思可以明确，我国没有也不应将网络平台视为宪法约束对象，应坚持在部门法框架内调整网络平台私益冲突。

4. 探究《数字服务法》的有效性以及该法规下代表协会的作用（Krzysztof Pacuła）

来源：ERA Forum: Journal of the Academy of European Law, Vol.25, Issue 2 (2024)

《数字服务法案》（DSA）解决了在线中介服务发展带来的挑战，并不可避免地带来了有关其运营的大量法律问题。虽然欧盟法院在附带程序中作出的第一批裁决必须在其作出的具体背景下进行解读，但这些裁决可以作为未来关于更广泛理解《数字服务法》的讨论的一个值得注意的参考点。这些裁决的一个有趣之处在于，它们有可能说明未来欧盟和国家层面的数字服务法案判例法中可能出现的两种前瞻性方法。

5. 欧洲征收数字服务税的五年：我们学到了什么？（Mateusz Kaźmierczak）

来源：Intertax, Vol.52, Issue 10 (2024)

本文旨在评估数字服务税（DSTs）是否有效地实现了其政策目标，确定关键的未解决问题，并强调欧洲五年来数字服务税存在的证据如何有助于解决这些问题。本文分析了数字服务税的主要政策目标，特别关注税收差距的均衡化和在税收发生率的背景下创造公平的税收。本文基于与引入五种选定的数字服务税相关的公开数据，这些数据基于其设计和引入国家经济状况的相似性。征收的收入、这些税的财政效率以及纳税人的反应强烈表明，数字服务税在很大程度上被转嫁给了中小企业和消费者，而产生的收入微不足道，这与他们的政策目标相矛盾。由于数据可用性的限制以及在分析期间发生的两次重大经济中断，一些问题仍未得到解答。因此，在理论经济文献适用于数字服务税的背景下，作者指出了在哪些方面需要对数字服务税进行额外的深入研究和政府分析，以及在引入类似措施方面获得足够的政治决策依据的可能方法是什么。

6. 数字市场法案和数字政策调查：最具创新性的监管工具之一的一周年应用观察（2023-2024）（Rezzi Ingemarsson & Pierre Bichet）

来源：Journal of European Competition Law & Practice, Vol.15, Issue 5 (2024)

《数字市场法案》是第一批全面规范世界上最大的数字公司的看门人权力的监管工具之一。无论是在内容上还是在程序上都是一项创新。该调查还对《数字市场法案》实施以来的数字监管和执法情况进行了比较分析。最终，《数字市场法案》将需要看门人有效地遵守，并由委员会忠实地执行，才能取得成功。

数字行政与司法

1. 法院“不当逮捕”的数字检察监督转型（吴进娥）

来源：《华东政法大学学报》2024 年第 5 期

法院“不当逮捕”是审判机关没有严格遵循逮捕要件而实施的逮捕，其不仅侵害被告人的程序性利益，还影响法官的中立性，可能给刑事诉讼结构带来毁灭性的冲击。传统以个案为基础的被动检察监督模式局限于卷宗审查、人工审查，对法院“不当逮捕”实施监督面临线索发现难、“不当”认定难、监督质效不突出等诸多瓶颈。为此，只有推动检察监督模式数字化转型，在法检之间建立一体化逮捕审查平台，探索建立法院“不当逮捕”智能算法模型并构建溯源监督机制，才能从个别、偶发、被动监督转变为全面、系统、能动监督，全面提升法院“不当逮捕”检察监督的效力。

2. 大数据预测警务的运作机理、风险与法律规制（陈永生）

来源：《中国法学》2024 年第 5 期

大数据预测警务的出现使警方侦查破案、预防和打击犯罪的能力获得突破性提升，但同时也会产生一些风险，须对其予以规制。域外预测警务已经过 1.0、2.0、3.0 三个阶段，预测能力不断提升，运作机理逐步优化。大数据预测警务的发展面临双重风险：一是数据的准确性、完整性和新鲜性难以保证；二是算法的错误、歧视难以避免和纠正。应当从三个方面对大数据预测警务进行规范：一是规范数据采集和处理的程序，确保数据的质量；二是建立算法审核机制，对算法的准确性和风险进行监督和评估；三是规制预测警务系统的设置与使用，确保对公民权利的保障。

3. 对司法智能化应用局限性的观察与思考——以民事司法智能化应用为中心（张卫平、冉博）

来源：《财经法学》2024 年第 5 期

司法智能化在我国司法实践中已经得到较为广泛的应用，并且随着人工智能技术的发展，司法智能化的实践将更加普及和丰富。司法智能化的运用对于提高司法的效率以及公正性都具有重要的意义，但也应当意识到司法智能化的运用也存在着

若干局限，必须对此有充分的认识，以免其盲目扩张和极端化，导致对既有制度发展和完善的抑制和阻碍。从目前司法智能的运行实践来看，其局限性主要体现在以下几个方面：第一，司法智能化大数据运用与案件审判中因果关系的龃龉；第二，司法智能化对司法自由裁量的弱化；第三，司法智能化运用中司法政策适用的困境；第四，司法智能化运用中政治、伦理等因素考量的障碍。

虚拟财产

1. 网络店铺转让的权属及其变动规则（杨立新）

来源：《清华法学》2024 年第 5 期

网络交易平台上的网络店铺的属性是虚拟不动产，其权属结构为“四权分置”，包括网络交易平台提供者的所有权、平台提供者与店铺经营者之间的债权、网络店铺经营权和网络店铺名称权。以不同的视角观察研究网络店铺转让会得出不同的结论，因而产生对网络店铺转让性质的重大争议。四权分置的基础权利是平台提供者的所有权，平台提供者和店铺经营者之间的债权是核心权利，经营权和名称权归店铺经营者享有。转让网络店铺的核心权利变动是债权债务概括转移，带动经营权和名称权的共同转让。网络店铺转让受合同自由原则约束，应当允许依法转让，关键要完善网络店铺转让的权利主体变动规则。

2. 数字财产权对传统财产权理论的重构（孙建伟）

来源：《中国法学》2024 年第 5 期

比特币、NFT 等数字资产的兴起以及数据资产入表改变了财产的界定和运行规则，对传统财产权理论提出了挑战，亟待重构数字时代的财产权理论。数字财产权是基于数字技术而产生的、对数字财产享有的财产权利，其核心在于对数字财产的支配和控制，系特定法律主体基于占有具备财产属性的数据而享有的权利，旨在赋予数字财产占有者在免受他人干扰的情况下使用其控制的数字财产的资格与能力。构建数字财产权规范体系，不仅要考虑中国特有的社会文化背景和法律传统，还需要国际合作和法律协同，以适应数字经济的全球化发展需求。《民法典》第 127 条为构建数字财产权的规范体系奠定了重要基础，在此基础上推进制定一部专门的《数字财产法》具有重要意义。

3. 论数字产品及其给付规则——以数字内容与数字服务区分为中心（吴逸越）

来源：《财经法学》2024 年第 5 期

《民法典》第 512 条第 2 款致力于规制数字产品的给付，但是仅提供了初步的不成熟的解决方案，且忽略了数字服务这一重要类型，无法应对当前数字社会的现实，更没有给数字经济与数字产品的未来发展预留空间。因此，必须重构数字产品的给付规则。根据数字内容和数字服务这两大类型的区分以及各自的技术特征和发展趋势，应当重点把握给付的标的物、向谁给付以及给付的具体方式这三个环节，分别确立数字内容和数字服务的给付规则。以给付数字内容为标的的合同本质上更接近于往取之债，而非赴偿之债，其给付完成的标志为经营者使消费者直接或通过其指定的其他系统可以获取数字内容或获得数字内容的方法；而对提供数字服务来说，经营者使消费者直接或通过其指定的其他系统可以使用数字服务即为完成给付。

（技术编辑：卞龙）

教研活动

中国人民大学法学院“新科技革命与未来法治创新团队”入选“教育部哲学社会科学创新团队建设名单”

日前，教育部办公厅公布首批“教育部哲学社会科学创新团队建设名单”，中国人民大学副校长王轶担任首席专家的“新科技革命与未来法治创新团队”入选。

教育部哲学社会科学创新团队建设工作是贯彻落实习近平总书记关于哲学社会科学的重要论述和在全国教育大会上的重要讲话精神的重要举措，是服务国家重大战略需求、推动建构中国自主知识体系的工作抓手。

中国人民大学获批的“新科技革命与未来法治创新团队”是跨法学、计算机科学与技术、人工智能、统计学、经济学等学科领域的综合性研究团队。团队聚焦新一轮科技革命为法学领域带来的挑战及社会发展中的重大法治前沿问题，积极促进法学与当代科技发展及司法实践的紧密结合与交汇融通，建构对新科技革命理论问题具有回应能力、对中国法律实践和法律体系具有解释力、对国际学术发展具有影响力的研究和教育团队，已形成了学科深度交叉、服务国家战略、处于国际前沿的研究特色。团队率先成立未来法治研究院，设立数字法学二级学科，建构法律与科技的中国自主知识体系，发起成立全国高校数字法学联盟、国际数字法学协会，联合成立全国唯一智慧检务创新研究院，为推动学科建设作出了突出贡献。

未来，“新科技革命与未来法治创新团队”将立足学术前沿，以重大理论研究问题和法治建设需要为导向，积极打通法学与计算机科学、人工智能、统计学、经济学、管理学等各学科的边界，聚焦新科技革命与法治形态的变革研究、网络法学研究、大数据法学研究、人工智能法学研究、智慧法治学科交叉研究等主攻方向。从数字法治的领域性、交叉性、横断性、可问责性等切入，面向数字法治与数字社会发展、数字法治与智能社会风险预防等多元政策议题之间的结合方式，数字法治与前沿科技之间的互动关系，数字法治与数字时代法律部门的组成形态，数字法治如何回应新型数字权力等关键议题，构建中国特色社会主义数字法治理论体系。在强化数字法治理论研究的基础上，形成面向国家战略需求的“大成果”与“大项目”，深化新科技领域与数字法治的交叉研究，将数字法治作为科技进步的坚实法律保障，实现法治与科技的深度融合与协同发展，回应中国式法治现代化对法治创新与科技发展的迫切需求。

此次获批既是团队长期深耕数字法治研究的结果，也是学校精心规划、持续培育的成果，标志着新一轮科技革命的背景下，中国人民大学在中国特色社会主义数字法治理论体系、学术体系、话语体系的建设上取得了重要进展。

张新宝教授应邀为云南大学法学院师生作主题为“数字法学基本问题”讲座

2024 年 9 月 21 日，云南大学法学院邀请中国人民大学法学院张新宝教授于法学院国际报告厅作“数字法学基本问题”主题讲座。

云南大学法学院院长陈云东教授担任本次讲座主持人。

讲座开始，张新宝教授首先指出，数字法学是近年来法学学科主动适应数字时代发展而出现的产物，其得名是因为该称呼具有最小颗粒度和最大包容性。张新宝教授表示，如果我们要想对数字法学进行认识就需要先掌握好网络、信息、数据等与数字法学相关的基本概念。随后，张老师便以目前汽车自动驾驶技术中所涉及到的数据合规、数字经济问题为例，帮助同学们对数字法学进行了初步理解。

接着，张新宝教授根据新闻热点以及自己的生活实际向大家提炼出了数字法学的学科特征：文理交叉学科、法学综合学科、国内国际统筹的涉外学科。

随后，张老师向大家展示了目前该学科的研究

热点，如网络安全与网络主权、数字政府、数字司法与智慧检务、网络治理、个人信息保护、数据财产权与数据要素的利用、电子商务平台的法律地位与责任、数据跨境流动以及人工智能立法与合法合规等课题。张老师结合热点新闻和具体案例阐释了该学科的涉及范围和发展前景，从国家立法、国家政策等方面解释了当前数字法学发展的基本情况，简要介绍了数字法学的基础理论以及数字经济法治、数字科技法治，令在场同学受益匪浅。

在互动环节中，张新宝教授与同学们亲切地进行交流并结合本次讲座的知识对同学们的问题予以详细回答

讲座回顾 |Anupam Chander：全球人工智能监管竞赛

2024 年 9 月 25 日上午，受中国人民大学未来法治研究院、中国人民大学法学院数字法学教研中心邀请，美国乔治城大学法学院教授、国际数字法学协会创始成员 Anupam Chander 教授出席中国人民大学未来法治研究院“全球荣誉讲席系列讲座”、中国人民大学法学院数字法学教研中心“数字法学系列讲座”，并围绕“全球人工智能监管竞赛”为主题发表了精彩的主题演讲。在演讲中，Chander 教授从“人工智能监管应以互联网监管的大背景为鉴”出发，探讨了法律在促进或者阻碍创新方面起到的关键作用以及欧盟人工智能法律规制的演进，并对知识产权法、隐私法对生成式人工智能起到的特别作用进行了深入分析。

美国乔治城大学法学院 Madhavi Sunder 教授，中国人民大学法学院副教授、未来法治研究院执行院长张吉豫，中国人民大学法学院教授、未来法治研究院副院长丁晓东，中国人民大学法学院副教授喻文光，中国人民大学法学院助理教授刘洋等出席本次讲座。本次讲座由丁晓东教授主持。

讲座的线下会场

在讲座开始之前，丁晓东教授对 Chander 教授表示热烈欢迎。丁晓东教授详细介绍了 Chander 教授的学术著作，并表示对此次讲座表示期待。在致辞中，他对 Madhavi Sunder 教授等与会嘉宾的热情参与和支持表示衷心感谢，并希望能够通过交流加深学术了解、增进学术共识

丁晓东

中国人民大学法学院教授

第一单元：主题演讲

Anupam Chander

美国乔治城大学法学院教授

Anupam Chander 教授对中国人民大学未来法治研究院、中国人民大学法学院数字法学教研中心的邀请表示衷心感谢。他对于能够参与此次“全球

荣誉讲席系列讲座”、 “数字法学系列讲座”学术交流活动感到荣幸。同时，他期待在未来进一步加强与人民大学的合作关系。

在随后的主题演讲中，Chander 教授从“人工智能监管应该以互联网监管的大背景为鉴”这一论点出发，探讨了世界范围内法律应该如何规制人工智能这一议题。Chander 教授指出，之前的经验告诉我们法律在促进或者阻碍创新方面起到了至关重要的作用；具体来说，法律能够塑造创新的类型，知识产权法、隐私法和侵权责任法对数字创新的特殊作用。

Chander 教授进一步指出，在互联网时代，法律规制创新是为了保护公共利益，包括消费者安全和消费者权利；知识产权保护对于促进创新和激发创造性来说十分重要，但知识产权中的例外情况同样会促进创新、并激发创造，正如他在《How Law Made Silicon Valley》一文中强调法律既能造就产业，也能摧毁产业。

纵观欧盟关于人工智能的立法进程，Chander 教授认为，欧盟担心自己有可能在人工智能时代再一次被甩在后面，于是它开始寻求制定既能促进创新，又符合基本权利保护的规则。其制定的规范的具体特征包括（1）基于风险的框架，（2）惩罚力度大（最高可达上一年度全球收入的 7%）（3）施加给“基础模型”（即《人工智能法》所称的“通用人工智能模型”）提供者的特殊责任。他进一步指出，欧盟最新的一系列数字立法均呈现出按照受监管实体的规模大小进行分别治理的态势，大型企业与小型企业所承担的义务不同。在《数字市场法案》(Digital Market Act)中，有专门针对“守门人”(Gatekeeper)的特别义务条款，而《数字服务法案》则对超大型在线平台或超大型在线搜索引擎进行了特别规定，《人工智能法案》(AI Act)则突出了构成“系统性”风险的通用人工智能系统这一概念。

之后，Chander 教授在指出欧盟《人工智能法案》的“未来面向”这一特性的基础上，探讨了这部法案对于通用人工智能模型产品的深远影响，并通过生动的案例深入浅出地引出了“人工智能领域正充斥着法律碎片化现象”这一论断。

最后，针对生成式人工智能领域，Chander 教授分别讨论了隐私法案、版权诉讼对于生成式人工智能发展与创新所带来的挑战，如 GDPR 中规定的数据最小化(Data minization)、透明度(Transparency)、数据处理的合法性基础(the legal basis for data processing)等要求将会使得生成式人工智能服务提供者举步维艰。同时，Chander 教授指出，需要密切关注美国法院有关生成式人工智能版权争议的判决，这或将决定未来十年的美国和欧洲人工智能创新的方向。

第二单元：嘉宾与谈

张吉豫

中国人民大学法学院副教授

张吉豫副教授首先对 Chander 教授的精彩讲座以及对人大法学院长期以来的支持表示感谢。中国目前正处在选择人工智能规制方向的关键时刻，其中规制的主要目的之一是促进创新，确保人工智能的可信度和积极影响。因此，需要考虑两个核心问题：一是中国立法应该解决哪些问题？二是如何更有效地解决这些问题？特别是如何在技术和市场之间实现长期协调，并在规范人工智能方面发挥积极作用。首先，可以考虑适当消除一些阻碍创新的现有法律限制。其次，需要对监管路径进行明智的选择。

喻文光

中国人民大学法学院副教授

喻文光副教授指出，为赢得人工智能时代的竞争优势，世界大国之间针对人工智能的立法和监管

竞赛日益加剧，但这会与全球人工智能治理产生矛盾冲突，因为后者需要各国合作以及更加协调一致的国际行动。如何协调全球人工智能监管中竞争与合作之间的矛盾关系，是人工治理监管与治理面临的重大挑战。此外，面对如何平衡创新与发展的监管难题，不同国家发展了各自的监管模式，例如美国更加倾向自我监管模式，而中国也在探索适合自己的监管模式。最后，由于人工智能技术及其应用的复杂性和持续发展的特性，如何对其进行恰当的定义是人工智能监管的另一大挑战和难题，而对人工智能的定义是人工智能立法和监管的前提，因为它决定了监管的范围和程度。不恰当的定义也会影响人工智能的创新和发展。

刘洋

中国人民大学法学院助理教授

刘洋助理教授指出，第一，人工智能监管竞争对监管竞争的理论有挑战。当前人工智能的监管与美国对此问题的国家安全化息息相关。特别是在对涉及中国的人工智能相关产业进行监管时，基本立场是阻止数据甚至资金、技术和人才的流动。因此人工智能的监管不是典型的监管竞争问题，法域之间通过调整监管水平来争取资本和其他产业要素的流动。在这样的情况下，全球监管竞争到底是竞争什么，是与以往文献理论不同的问题。第二，目前对人工智能的监管竞争所称的目的“创新”，需要从政治经济的角度来理解。人工智能产业当前是资本密集，所以当前监管的促进创新，很大程度上是促进资本密集型的企业优势。理解这一点，才能理解中美欧等方面在监管立法基本立场上的差别。

Madhavi Sunder

美国乔治城大学教授

Madhavi Sunder 教授是知识产权、法律与文化领域的知名学者。她于 2006 年被任命为卡内基学者（Carnegie Scholar）。她曾担任耶鲁大学法学院、芝加哥大学法学院和康奈尔大学法学院的法学访问教授。

Sunder 教授指出，立法应当在促进创新和抑制创新可能带来的负面影响之间找到平衡。这需要我们回归基础理论，思考知识产权法的根本目的是什么。除了促进创新之外，我们还应该考虑社会利益、公共利益等价值。人工智能立法同样需要考虑其对消费者保护的影响，比如虚假信息和深度伪造等问题。因此，当前人工智能监管面临的问题可能并非全新的问题，它们可能是我们之前已经探讨过的问题。

在嘉宾与谈中，Chander 教授认为，中国人民大学法学院在数字法学领域的研究具有国际前沿性，他对各位嘉宾的评论和问题作了细致回应，回答了参与讲座同学们的问题。在两个小时的精彩主题演讲和深入与谈交流后，本次讲座圆满结束。主持人丁晓东教授对 Chander 教授、Sunder 教授和各位与谈嘉宾再次表示感谢，并宣布此次讲座圆满结束。

会议回顾丨新一代人工智能国家科技重大专项“可信人工智能立法制度建设研究”中期检查会顺利召开

2024 年 9 月 26 日，由中国人民大学副校长王轶教授担任项目负责人、中国人民大学牵头承担的新一代人工智能国家科技重大专项“可信人工智能立法制度建设研究”中期检查会在中国人民大学法学院顺利召开。

该项目由中国人民大学联合中国电子技术标准化研究院、华中科技大学、北京理工大学、西安交通大学、北京大学、中国信息通信研究院等 7 家单位共同承担。国家自然科学基金委员会高技术发展中心信息处项目主管、北京市科学技术委员会干部、项目中期检查专家组专家、项目负责人及项目成员等 30 余人参加了本次会议。

北京航空航天大学吴文峻教授、北京邮电大学杜军平教授、北京工业大学张建标教授、中国科学院信息工程研究所韩冀中研究员、北京交通大学朱振峰教授等 5 位专家组成专家组，对项目进行中期检查和指导。

首先，国家自然科学基金委员会高技术中心项目主管孟召宾，向指导专家介绍了专项总体情况、管理规范和流程以及项目中期检查要求。

接着，项目负责人中国人民大学副校长王轶教授就中期执行情况，从项目整体研究背景、项目研究进展、项目中期重点成果、项目组织管理情况等部分进行了汇报。

与会专家在听取项目汇报后，对项目中期成果给予了肯定性评价，并针对项目理论创新点的深化、项目指标落实及科技报告的具体情况、项目中期成果与下阶段成果的衔接等多个方面提出了完善建议。

随后，与会专家讨论并形成了中期检查意见，认为项目中期进展符合预期目标，顺利通过中期检查。

会议最后，项目负责人、中国人民大学副校长王轶教授向与会的领导和专家表示感谢，并代表项目组保证后续将根据专家建议对项目成果进行完善，以确保研究成果的深度和广度，为中国人工智能立法工作提供坚实的理论支撑。

论坛预告 | 第五届“未来法治与数字法学”国际论坛

数字科技有力推动着经济社会发展，深刻改变着人们的生产生活方式。习近平总书记指出：“发展数字经济意义重大，是把握新一轮科技革命和产业变革新机遇的战略选择。

党的二十届三中全会提出“加快构建促进数字经济发展体制机制”并作出重要部署，为推动数字经济进一步发展指明了方向。未来法治探索和数字法学研究，与我国国家战略紧密相连，是数字中国建设和法治中国建设双重战略框架下，法学领域的重要使命和责任。

为进一步推动未来法治与数字法学领域的研究，加强未来法治与数字法学领域的国际交流与合作，为全球数字经济高质量发展做出积极贡献，中国人民大学法学院、吉林大学理论法学研究中心与京东集团联合举办第五届“未来法治与数字法学国际论坛”。本次论坛的承办方为中国人民大学未来法治研究院、吉林大学理论法学研究中心、京东法律研究院和司法文明协同创新中心，支持单位为人民法院出版社《数字法治》编辑部。

论坛诚挚邀请国内外知名专家学者、政府机关领导、著名法官及产业界代表与会，惠赐高论，切磋碰撞，凝聚共识，以期具有前瞻性、多维度地研讨未来法治与数字法学领域的法治命题与创新，为社会发展贡献力量。

论坛时间及单元主题

地点：北京市海淀区

2024 年 11 月 1 日：办理入住及签到

2024 年 11 月 2 日：第一单元—第四单元

2024 年 11 月 3 日：第五单元—第六单元

第一单元：主旨演讲

第二单元：院长圆桌会议

第三单元：数字法学的理论发展

第四单元：未来法治的前沿探索

第五单元：数字经济发展与法治保障

第六单元：数字平台与人工智能治理

报名链接：

（技术编辑：张锦涛）

数字法评

赋能型人工智能治理的理念确立与机制

原载：《中国法学》2024 年第 5 期，第 61-81 页

作者：张吉豫

摘要：人工智能治理已成为国家和社会治理的前沿问题和重要领域。然而，当前在人工智能科技创新、风险防控、企业自治、政府监管、社会监督、国际协作等方面都亟需加强能力建设，必须把提升人工智能安全可信发展的能力作为人工智能治理的第一要务，构建“赋能型人工智能治理”的理念和机制。以此为目标，应坚持以人为本、发展导向的赋能型人工智能治理核心理念，以及从中发展出的智能向善、包容审慎、敏捷治理、可持续发展等基本理念。应建设以法治为核心的赋能型人工智能治理机制以及法治统领下的各项具体机制，如完善法律治理与技术治理相统合的机制，建立多元主体沟通协作的共治机制，构建与人工智能发展相适配的“避风港”机制，建立敏捷互动、激励向善发展的动态监管机制，建设人工智能安全保险等社会保障机制。

一、引言

21 世纪以来，人工智能技术迅猛发展，正引领新一轮产业革命，日益成为决定国家竞争力和国家安全的重大战略性技术，同时其广泛使用也给人类带来全新的风险挑战。这使得人工智能治理成为国家治理体系的重要组成部分。党的二十届三中全会通过的《中共中央关于进一步全面深化改革推进中国式现代化的决定》（以下简称《决定》）指出，“完善推动新一代信息技术、人工智能、航空航天、新能源、新材料、高端装备、生物医药、量子科技等战略性产业发展政策和治理体系”[1]。如何科学有效进行人工智能治理，树立什么样的治理理念，建构什么样的治理机制，形成什么样的治理格局，无疑是法学界和科技界必须回答的时代之问和世界之问。

2024 年 7 月 1 日，第 78 届联合国大会协商一致通过中国主提的加强人工智能能力建设国际合作决议，140 多国参加决议联署。[2]这充分反映了当前人工智能能力建设的重要意义。对此，本文从不发展是最大的不安全、不充分发展是最大的隐患等判断出发，指出人工智能的安全可信是一种需要建立在高发展水平基础上的能力，并针对现阶段亟需能力建设的切实情况，提出“赋能型人工智能治理”的概念。本文将在论述赋能型人工智能治理理论依据的基础上，指明赋能型人工智能治理的核心理念和基本理念，并提出健全以法治为核心的赋能型人工智能治理新机制。赋能型人工智能治理新理念和新机制的结合，必将形成人工智能治理新范式新格局。

二、赋能型人工智能治理的理论依据

以人工智能为首的新兴科技正有力推动着社会各个领域的迭代升级，将在中国式现代化进程中发挥至关重要的作用。在此背景下，2024 年《政府工作报告》明确提出开展“人工智能+”行动的工作规划。[3]人工智能将日益广泛地应用在社会生活和国家治理各个方面。随着应用领域和影响力不断扩大，人工智能系统的潜在风险也逐渐凸显。这对人工智能治理提出了促进发展和保障安全的双重需求。现代社会的运行和人的发展建立在信任基础之上，而信任又是建立在对系统的可依赖性的信心之上。[4]社会需要引领和保障人工智能的安全可信发展。

在迈进智能时代的关键历史时期，人类社会需要形成与时代相匹配的运行能力，然而，当前人工智能企业创新发展能力、风险识别和防控能力、政府监管能力、社会监督和正确应用人工智能的能力、国际协作能力等都存在明显不足，缺少充分的信息和成熟的治理经验，社会治理面临全新的挑战。应

当看到，这样的挑战是人工智能这种引领产业革命的颠覆性、战略性科技发展初期所必然产生的。创新发展、风险防控等能力不可能凭空获得，需要在发展过程中积极建设。可以说，当前人工智能发展中的主要矛盾，是人工智能安全可信发展的巨大需求与人工智能发展及治理能力不足之间的矛盾。面对这种复杂情景，有必要创新人工智能治理理念和机制，将解决人工智能安全可信发展的能力缺口作为治理要解决的重点问题。因而，在回答我国需要什么样的人工智能治理机制时，首先要明确当下的治理目标，即通过科学治理来赋能人工智能安全可信发展，使得人工智能科技与社会治理能力同步提升，最终使社会建立起可以在人工智能时代良好运行的能力，让人工智能真正服务于人民幸福和人类福祉的提升。因此，本文提出建构着眼于社会能力提升的“赋能型人工智能治理”，具体理据包括如下方面：

（一）人工智能所处的发展阶段

在动态的社会技术变革过程中，科技发展、治理模式与规范观念之间存在相互作用。[5]治理模式的确定需要把握科技规律、经济规律和治理规律，符合所处发展阶段的特征和需求。当前我国人工智能发展的阶段性特征对人工智能治理模式提出了基本要求。

首先，我国人工智能发展处于世界前列，缺少可以借鉴的成熟治理经验。过去我国在许多领域的发展晚于发达国家，可以参考国外在实践中产生的信息经验来进行科学决策。然而，随着我国人工智能科技进入世界领先行列，从“跟跑”变为现在的“并跑”乃至在一些方面的“领跑”，几乎没有经过实践检验的成熟治理经验可以借鉴。“传统政策工具进入信息‘盲区’，这是更好发挥政府作用面临的严重挑战。”[6]在此情况下，需要坚持对人工智能新业态新模式的包容和普惠赋能，升级治理模式和治理能力，加强及时获得风险信息、治理机制及其能效信息的能力建设。

其次，当前人工智能仍处于高速发展阶段，并可能出现难以预测的突破性进展，这也使得传统基于充足信息的静态化治理机制难以有效适应人工智能发展。正如 2022 年末基于大模型的人工智能发展，使得当时已经形成较高程度共识的欧盟《人工智能法案》受到挑战，不得不进行修改，专门增加了一章针对通用人工智能模型的管理要求。[7]这突出反映了该法案当时的局限性，体现了相对静态的治理机制回应技术发展的能力不足，因而需要建设更为敏捷动态的治理机制，以增强对变化迅速的科技发展的回应能力。

再次，当前人工智能虽然取得了显著进步，但整体而言仍处在发展早期。科技界对于大模型“智能涌现”现象的理解仍不透彻，[8]用于保障人工智能安全和伦理价值对齐的技术发展更是非常不充分。这种阶段性特征一方面决定了无法要求人工智能立即达到理想的安全可信状态，另一方面也提示我们不能仅以当下的人工智能发展情况来进行评价，而是应该以动态的、发展的眼光来进行系统研判，特别是重视和推动科研群体及掌握先进科技的人工智能企业不断发展技术能力，以不断解决发展中存在的风险问题。

最后，我国人工智能发展虽处在世界前沿，但仍落后于美国。过往的百余年历史让我们深刻体会到科技发展对国家命运的重大影响。面对国际人工智能科技发展可能带来的影响，自身科技的高度发展是维持国家竞争力和国家安全的根本能力。因此，我国必须重视赋能人工智能发展以及安全能力的提升。

综上所述，当前我国人工智能发展的阶段性特征决定了需要赋能型人工智能治理。过去那种通过借鉴先发展国家的经验、在相对充足的信息基础之上进行静态规则制定和治理的模式难以适应当前的人工智能治理需求，应当在包容和普惠赋能的基础上，发展敏捷动态的治理机制和提升治理能力，特别是注重赋能人工智能合规科技、监管科技的同步发展，以不断提升安全能力。

（二）人工智能发展的机遇与挑战

人工智能是引领未来的战略性技术。许多国家都积极抢抓人工智能发展的战略机遇，构筑人工智

能发展的先发优势。我国在 2017 年发布了《新一代人工智能发展规划》（国发〔2017〕35 号），以此牵引创新型国家和科技强国建设。在党中央科学决策和国务院规划部署下，我国人工智能产业发展迅速，处于良好的战略机遇期。但同时也要看到，我国人工智能发展还面临一系列挑战。美国在新一轮人工智能发展中仍处在引领地位。根据斯坦福大学发布的研究报告，美国 2023 年在人工智能领域的投资位于世界首位，高出中国将近 8.7 倍。[9]由于新一代人工智能仍处于发展初期，其创新发展和应用存在很大的不确定性，依赖数据、算法、算力、产业生态环境、营商环境和社会应用环境等多重因素，人工智能投资必然是高风险活动。只有当期望收益高于期望成本时，理性投资人才可能对创新进行投资。[10]如果人工智能创新活动的成本收益衡量缺乏稳定的良好预期，企业会对重要的投资和研发信心不足，面临是将资金投入人工智能科技还是其他项目的选择。供应链可及性和稳定性、进入市场的门槛、知识产权保护情况和竞争环境等营商环境因素都是市场主体在制定规划时需要考虑的制度要素和社会条件，是国家治理能力、体制机制、社会环境等因素的综合反映。[11]

习近平总书记强调，“科技领域是最需要不断改革的领域”“推进自主创新，最紧迫的是要破除体制机制障碍，最大限度解放和激发科技作为第一生产力所蕴藏的巨大潜能”。[12]从国内来看，还存在一些制约人工智能发展能力的制度问题。第一，在数据汇聚利用方面，目前法律制度中还存在机器学习合理使用规则缺失、反不正当竞争法适用中对数据爬取利用过度限制、公共数据流通利用规则不明确不统一等问题。[13]第二，人工智能产业发展仍存在一些领域市场准入困难、试验区域有限、法律规则模糊、规制成本偏高、侵权责任过重等问题，需要进行责任科学界定和监管机制优化。第三，人工智能创新的知识产权保护制度尚不完善，对于积极研发人工智能价值对齐机制及规制技术的企业缺少有效激励机制。[14]第四，由于一些人工智能应用曾出现安全风险、算法歧视、泄露个人信息、损害劳动者权益等问题，加上社会公众对失业和科技异化的担忧、风险防御能力和监管能力不足等现状，影响了社会对于人工智能的信任，[15]限制了人工智能的应用。此外，从国际上看，美国等一些国家以所谓的“国家安全”名义打压中国信息科技企业，限制其产品和服务，不断升级对中国的芯片出口限制，试图遏制我国在人工智能等前沿科技领域的创新发展，也使我国当前人工智能发展面临严重挑战。

无论是利用好战略机遇，还是应对国内外挑战，都迫切需要面向人工智能发展中能力不足的问题要点，构建赋能型人工智能治理机制，为人工智能创新发展提供更加有利的制度条件，为企业投入人工智能创新提供激励和更加稳定的制度预期。同时，在涉外法治建设中，应建立健全能够有力应对外国遏制和打压的新机制，以此提高我国参与全球人工智能治理体系建设的能力，助力我国人工智能企业和行业抢占创新发展的制高点，为中国式现代化提供强大的科技支撑。

（三）人工智能风险的基本特征

随着人工智能的应用领域不断扩大，人工智能的潜在风险也日益受到社会关注，很多研究对人工智能的风险问题和应对措施展开了积极探索。[16]在构建人工智能风险治理机制时必须注意，人工智能带来的风险具备现代社会意义上公共风险的一些共同特征。

首先，人工智能风险具有公共性和规模性。这种现代社会的公共风险在很大程度上超出了个体风险承担者的直接理解和控制。[17]公民个体通常欠缺对这种公共风险的认知能力、预防能力、谈判能力，因此往往难以在充分理解风险的基础上做出理性选择，完全由公民在意思自治的基础上自担风险的合理性基础被动摇，带来了政府介入和依法治理的必要性。

其次，人工智能风险具有两面性。任何一种创新活动都伴随着未知，在带来风险的同时，也提供着新的发展机遇。吉登斯描述了既包括机会与创新，也包括安全与责任的“风险矩阵”。他指出，“风险不只是某种需要进行避免或者最大限度地减少

的负面现象；它同时也是从传统和自然中脱离出来的、一个社会中充满动力的规则”；“机会与创新是风险的积极一方”，“对风险的积极参与是社会与经济动员的一个必要成分”。[18]例如，辅助驾驶和自动驾驶技术在可能带来新型交通事故风险的同时，也可能极大减缓因人类驾驶员的疲劳驾驶、反应迟缓等情况造成的风险，从总体上提高交通安全。[19]因此，对风险的态度伴随着价值判断，融合着针对一个事物或行为的收益和损害所进行的判断和比较。在对损害可能规模发生之概率的理性计算的基础上，风险可能成为提供给人们的机会。[20]我们要以辩证观念和辩证思维正视人工智能风险的两面性，促进科技创新对社会的正面价值和积极意义。

最后，人工智能风险具有一定的可控制性。人工智能带来的风险是一种“人为风险”。社会之所以允许这种人为风险存在，一方面是因为其具有两面性、能带来促进社会发展的积极意义；另一方面是因为人们相信这种风险在很大程度上能够通过对于人们活动的引导和规范来从结构上得到控制，社会可以通过有意采取的预防性行动以及制度化措施克服发展带来的副作用。[21]现代社会生活具有反身性。社会实践总是不断受到关于这些实践本身的新认识的检验和改造，从而在构成上不断改变着自己的特征。[22]我们应努力提升认识和防控人工智能风险的能力，将其作用于社会并改变风险的样态。

从人工智能风险的特征和发生及控制规律的认知出发，我们“需要抵御风险的保障，但也需要具有面对风险并以一种积极的方式来对待风险的能力”[23]。风险的两面性决定了治理目标的双重性。我们需要关注风险中蕴含的机遇，通过实施赋能型治理，在发展中提升社会认知和防控人工智能风险的能力，使得人工智能发展成果切实服务于人类福祉的提升。

（四）人工智能治理能力的现存缺陷

当前社会在人工智能风险的认知和评估能力、社会监督能力、企业内部自治能力、政府外部监管能力等方面普遍不足，需要以“赋能”为核心，加强人工智能时代所需要的治理能力建设。

首先是对人工智能风险的认知和评估能力不足，社会监督能力欠缺。全面认识和把握人工智能风险是进行风险治理的重要基础，但由于人工智能的风险信息不充分、不及时，企业、社会公众、政府主管部门等各类主体往往对人工智能新技术新应用的风险缺乏清晰认知，以致出现对人工智能风险产生掉以轻心或过度恐惧的两极分化。目前，存在对人工智能风险的认知、评估和监督的能力缺陷，主要有三方面原因：一是人工智能自身的复杂性。人工智能具有“黑箱性”、一定程度的“自主性”、运行结果的难预测性、运行机理的难解释性、可能根据环境变化的自适应性以及高速迭代更新发展等特性，这些都为风险认知、评估、监督和防控提出了挑战。二是人工智能的社会应用广泛。人工智能广泛应用在社会生活的方方面面，其风险识别和评估不仅需要人工智能科技专家参与，还需要应用领域的专家、法学家、伦理学家、社会学家等共同参与，以更全面地评估人工智能在整体上以及具体场景中所产生的影响。三是数字鸿沟问题加剧。当前社会公众对人工智能的理解和运用能力差别非常大，这既影响到人工智能科技的普惠应用，也使得欠缺理解的群体在人工智能风险面前更为脆弱。这三方面都决定了需要面向人工智能治理进行针对性的能力建设。

其次是企业对人工智能风险的自治能力不足。企业作为人工智能的主要研发者、部署者，具有在其研发部署过程中针对可能的风险采取自我治理的机会。然而大量企业特别是中小微企业的自治能力有限，缺少必要的技术措施和管理措施储备，往往难以将人工智能伦理规范和治理原则转化为有效的具体措施。当前，能够提升人工智能的安全性、准确性、稳健性、可解释性、公平性、包容性等的技术还需要大力创新发展，加上技术的研发和实施成本过高，企业也往往怠于自治。还有许多人工智能企业算力资源不足、高质量训练数据欠缺，这也制约了企业有效自治的能力。

最后是政府科学监管和促进发展的能力不足。一方面，科学有效的监管需要理论支撑、机制建设和技术赋能。关于人工智能发展情况及规律、人工智能风险以及有效的风险治理方法的信息不充分、不对称，加上资源不足、工具匮乏等问题，使得政府监管方式的可操作性、有效性和合理性都容易受到质疑和挑战。面对新兴科技的新型治理理念的实现，更加需要国家的基础设施与行政能力予以辅助，包括信息汇集与科学分析能力、风险判断能力、吸纳市场积极要素的能力等。[24]另一方面，从政府角度促进人工智能发展也亟待能力建设。算力、数据等要素以及测试、评估、认证等服务的提供都需要必要的制度支撑。政府推动人工智能在民生服务、社会治理、经济发展等领域的融合应用也需要建设相匹配的新型风险治理能力，以保障其可持续发展。

因此，针对人工智能治理的现存缺陷，必须构建赋能型治理，建设高水平治理能力，以此推进人工智能高质效地安全可信发展。

（五）既有人工智能规制模式的局限

既有的规制模式和理论，为人工智能治理提供了有益参考。但面对新一代人工智能发展态势，其局限性逐渐显露出来。

既有规制模式主要包括命令—控制型规制、建议劝服型规制、回应型规制、元规制等，可从规制者、规制对象、命令类型和后果类型等方面考察其差异。[25]命令—控制型规制通常事先制定具体的特定命令，而违反的后果通常是比较强的制裁。但理想中这种模式下的命令应具有较高的规则精确性，在人工智能仍高速发展的当下难以实现。建议劝服型规制模式主张建立合作而非对抗的局面，[26]命令形态往往是一般性的目标，主要依赖企业自我规制，但在企业利益驱动面前往往效果大打折扣，在人工智能领域更是存在算法黑箱等诸多问题。[27]因此，这两种规制模式都难以取得理想效果，以致陷入“科林格里奇困境”[28]。许多研究者在这两极之间寻找更加综合性、动态性的规制模式。回应型规制旨在弥合强监管和放松监管之间的鸿沟，设想规制活动发生于对话式、交互性的环境中，规制者通常优先采用干预性较低的措施，但如果措施失灵，规制者就会逐步采取更具有惩罚性或强制性的措施。其最突出的特点即后果的动态回应性。[29]回应型规制模式可派生出很多具体形式，常与元规制相结合。[30]元规制即对企业自我规制的规制。政府通过提出一般性目标的命令来要求和塑造企业内部的自我规制，调动企业的主观能动性，让企业凭借自身掌握的信息和科技能力来制定适当的具体规范，[31]并由外部规制中的法律后果来提供行为激励。这种规制模式在数字科技领域得到了较多应用。但其成功条件在于，政府作为外部规制者需要建立获得风险情况、企业采取的规制措施的成本和实效、行业中相关技术发展水平等一系列关键信息的能力，并能够提供合理的惩戒和激励机制，才能在保障发展的同时有效地激励企业积极开展自我规制，同时企业也需要具有在合理成本内有效实施自我规制的信息、资源和能力，并要特殊考虑中小微企业的自我规制能力问题。例如，“信息对称性”原本是自我规制的重要优势，[32]但面对高速发展的人工智能，企业实际上也难以充分掌握人工智能新应用的风险情况和有效措施等信息。因此，这类规制模式在人工智能领域的适用对相关能力建设提出了更高要求。

上述各种规制模式形成了从最严格到最宽松的谱系，为人工智能规制提供了重要的基础，特别是在回应型规制和元规制模式的基础上，研究者们对寻找与人工智能治理相适配的规制模式进行了许多积极探索，[33]但在理念上尚缺乏对人工智能安全可信发展所亟需的各项能力建设的突出强调，即缺少对于“赋能”这一维度的着重考虑。在人类社会迈向智能时代、但安全可信发展能力尚待建设的现阶段，有效的规制状态不可能一蹴而就，需要从对基础的规制模式讨论升级至对能力建设的研究，明确“赋能”这一目标，实现良好规制的切实落地。

综上所述，当前人工智能产业发展需要赋能，形成安全可信的技术和保障体系更加需要赋能。安全不只是一种状态，更是一种能力。我国《国家安全法》将国家安全定义为“国家政权、主权、统一

和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力”。这种安全能力观在我国数字科技领域的立法中也得到突显。《网络安全法》将网络安全定义为“使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力”。《数据安全法》将数据安全定义为“确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。从这些定义中可见“能力”的重要性。同时，这三部法律也都明确了促发展的目标，这不仅是出于平衡考虑，更是因为真正的安全应该是也只能是建立在高度发展之上的安全。

在当下阶段，不发展是最大的不安全。人工智能治理的目标不是简单追求一个局部性、临时性的假性安全状态，而应该是追求达到一个拥有高度发达的科技水平和保障持续安全可信能力的状态，应以此为目标构建推动能力提升的有效治理机制。因此，赋能型人工智能治理的核心要义在于以赋能为核心，通过科学有效的治理，实现高度的人工智能发展水平和保障持续安全可信状态的能力，即针对人工智能安全可信发展中的重要能力建设需求，通过治理实现如下方面的赋能：第一，赋能企业创新发展，提高我国企业和人工智能行业整体竞争力，特别是增强发展要素的普惠赋能，包括对数据要素、算力要素、算法要素、制度要素的协同赋能。第二，赋能企业可信规制，特别是注重风险管理能力的普及发展，使得大中小型企业都能够开展有效的自我管理，从源头防控人工智能研发运用的伦理风险和安全风险。第三，赋能政府有效监管，特别是积极发展和推广用于人工智能治理的相关技术，实现人工智能治理技术的创新突破。第四，赋能社会公众平等受益于人工智能的发展，使社会公众有效地参与人工智能治理，提升社会公众对人工智能发展的信任度，营造有利于人工智能可信发展的社会环境。第五，赋能我国深度参与全球人工智能治理体系建设，为推进全球人工智能治理体系现代化提供中国经验、中国智慧和中国力量。

三、赋能型人工智能治理的理念确立

赋能型人工智能治理建设需要确立与之相适应的理念：既要确立核心理念，即明确如何理解赋能型人工智能治理中涉及的重要关系，从而为“赋能”确立正确的方向和界限；也要从核心理念中发展出基本理念，更为具体地指引赋能型人工智能治理机制的构建。

（一）赋能型人工智能治理的核心理念

赋能型人工智能治理的核心理念基于两大关系而形成，即人与物（智能体）的关系、发展和安全的关系。

1.坚持以人为本，促进人机和谐

将以人为本作为核心理念，明确了赋能人工智能安全可信发展的最终目标是赋能人民，为赋能型治理确立了方向和评价标准。以人为本是可信人工智能的基础，是人工智能治理的首要理念与终极关怀，体现为从人类福祉、人类安全、人的尊严和权利、人的全面发展出发，充分尊重和保障人权，确保人工智能解决方案是以人为主体、人工智能的使用以人为中心。发展人工智能归根结底是为全体人民提供优质的公共服务，确保人工智能技术成果平等普惠共享。

以人为本是全人类的共同价值。世界上人工智能发展和治理走在前列的主要国家的法律法规、政策文件、纲领宣言、伦理指南等几乎都将以人为本作为其核心理念和根本原则。在人工智能治理上，联合国和相关全球性峰会也都主张以人为本，如 2017 年发布的“阿西洛马人工智能原则”[34]、2021 年联合国教科文组织（UNESCO）第 41 届大会通过的《人工智能伦理问题建议书》、2023 年中美等 28 个国家在英国签署的《布莱切利人工智能宣言》、2024 年第 78 届联合国大会协商一致通过的中国主提的加强人工智能能力建设国际合作决议，等等。

我国在人工智能发展与治理上，更是始终坚持以人为本的核心理念。《民法典》《个人信息保护法》等法律法规，都充分体现以人为本的精神，注重对智能时代公民个人信息权益、隐私权、肖像权、

声音权、免受自动化决策权等的保护。2023 年 10 月 18 日，我国发布《全球人工智能治理倡议》，第 1 条就明确主张：“发展人工智能应坚持‘以人为本’理念，以增进人类共同福祉为目标，以保障社会安全、尊重人类权益为前提，确保人工智能始终朝着有利于人类文明进步的方向发展。”

以人为本不是空洞的理念标签，而是应当落地为人工智能治理的法治原则和法理话语，指引着赋能的核心方向。以人为本首先体现为以人的权利为本，尊重和保障人权；其次体现为公平正义，重视算法公平，注重数字无障碍设计，缩小数字鸿沟，实现普惠发展；最后体现为确保人类在人工智能运行中的主体性、自主性，实现“人在回路”（human-in-the-loop）控制、发展人机协同控制等方法，[35]确保人类能够始终实质性监督和控制人工智能。

2.坚持发展导向，统筹发展和安全

发展是人类社会的永恒主题。坚持发展导向，统筹发展和安全，是赋能型人工智能治理的另一项核心理念。

世界各国在人工智能治理中都须考虑如何平衡好发展与安全。欧洲议会在投票通过《人工智能法案》前的最后时刻仍在为如何平衡促进创新与防范风险这一问题辩论，凸显出如何处理好发展和安全的关系是人工智能立法的基本问题和工作难题。

在新时代中国式现代化进程中，发展和安全的关系演化为高质量发展和高水平安全的关系，要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。《决定》指出，“加快构建新发展格局，推动高质量发展”“建设更高水平平安中国，健全国家安全体系”“实现高质量发展和高水平安全良性互动”。[36]这为人工智能治理确定了根本遵循。要把这一核心理念贯穿到人工智能治理的各环节全过程，将安全与发展协同部署，构建有利于人工智能安全可信发展的生态系统。

正确认识和统筹人工智能发展和安全的关系，要从我国人工智能发展水平和治理能力出发，对人工智能战略问题开展前瞻性、针对性、储备性研究。发展是安全的基础。历史和现实都证明，“发展是解决我国一切问题的基础和关键”[37]。我国人工智能技术发展仍处于追赶阶段，在人工智能科技已经成为国家的核心竞争力乃至大国博弈实力的今天，人工智能不发展是最大的不安全，发展不充分是最大的风险隐患。保障人工智能安全可信的能力、保障人工智能时代国家和人民的重大利益处于持续安全状态的能力，只可能是建立在高发展水平基础上的。人工智能治理应为其创新发展留有充足的空间和时间。相关政策、法律制度应遵循和尊重新一代人工智能研发应用的规律和现实，以有利于人工智能发展和更好发挥作用为根本出发点，着力赋予权利、减轻义务、科学监管、提供服务，防止监管发力过猛对创新发展造成实质性损害。要把握未来发展主动权，增强我国人工智能的竞争力、发展力、持续力、安全力以及引领力。

安全是发展的条件和保障。没有安全机制和安全措施，人工智能的可信发展也无从谈起。人工智能治理的重要任务：一是划清安全底线；二是在发展中坚持总体国家安全观，推进人工智能全过程的安全保障体系和能力建设；三是坚持以共同、综合、合作、可持续的全球安全观为战略武器，反制一些国家对我国人工智能发展的遏压，打造安全屏障和安全环境。

坚持发展导向、统筹发展和安全的关系，要坚持良法善治，在法治轨道上促进发展和安全良性互动，切实做到人工智能产业发展与安全治理之间的稳定平衡，使之相辅相成，以安全可信的新一代人工智能技术推动产业升级和新质生产力发展。

（二）赋能型人工智能治理的基本理念

基于上述核心理念和国内外人工智能治理经验，赋能型人工智能治理理念可进一步展开为如下基本理念：

1.智能向善

智能向善既是以人为本理念的要求，也为统筹发展和安全指出具体路径，指引着对安全可信发展能力的不断建设。智能向善是科技向善、数字向善原则在人工智能科技领域内的具化。其核心是，推动从事人工智能研发、提供和使用活动的个人、企

业、行业等主体遵守社会公序良俗、社会主义核心价值观和全人类共同价值，向善发展和利用人工智能，满足人民群众美好生活对智能科技的需要，不断增进人类共同福祉；同时推动政府部门和社会组织对人工智能向善而治，防范恶意开发和应用人工智能技术，消除数字鸿沟，促进数字正义和社会公正，推动人类文明进步。我国发布的《全球人工智能治理倡议》特别提出“发展人工智能应坚持‘智能向善’”，其宗旨就在于此。

面向未来，确保人工智能技术开发应用遵循智能向善的理念，是人工智能治理的关键所在。首先，需要在以人为本、发展导向的核心理念引领下，不断完善对人工智能应用领域价值目标（“善”）的认识，并将“善”的目标加入人工智能研发的目标体系，在技术研发全流程中加以实现。其次，需要依托具体机制措施，推动人工智能科技向善发展，特别是推动能够支撑人工智能价值对齐、安全可信的技术措施和管理措施的创新与应用。各类科技的创新发展不是均衡的、步调一致的，要针对企业的“研究偏向”问题，[38]加强伦理和法治引导，保障企业在“智能向善”的轨道上运行。要在保障企业创新发展能力的同时，赋能有益于人工智能与社会伦理价值对齐的科技研发和管理制度创新。

2.包容审慎

包容审慎是坚持发展导向、统筹发展和安全理念的具化，有助于赋能企业创新发展，是我国在科技领域一以贯之且行之有效的先进理念，并体现在法律、行政法规和部门规章之中。《科学技术进步法》第 35 条规定：“国家鼓励新技术应用，按照包容审慎原则，推动开展新技术、新产品、新服务、新模式应用试验，为新技术、新产品应用创造条件。”2023 年，国家网信办等 7 部门联合发布的《生成式人工智能服务管理暂行办法》第 3 条规定，对生成式人工智能服务实行包容审慎和分类分级监管。包容审慎与科技赋能是辩证统一的。2024 年 3 月，李强总理在北京调研时指出，人工智能是发展新质生产力的重要引擎，要在守住安全底线的前提下，积极推行包容审慎监管，给予新技术足够的创新空间和必要的试错空间。[39]

包容审慎作为人工智能治理的一项基本理念，其要义在于，对人工智能新技术新产品新业态采取适度宽容的态度，允许其在守住安全底线的前提下自行纠正研发应用过程中出现的问题，政府在审慎跟踪观察的同时，只进行适时适度的干预。换言之，对人工智能新技术包括颠覆性技术的出现应当秉持积极拥抱、包容审慎的治理理念和规则策略，对其引发的新情况新问题，不必急于管制或惩罚，防止因监管失当而将其扼杀在萌芽状态。从传统规制理论角度观察，包容审慎监管映射出回应性规制的执法策略、合作规制的运行范式以及规制试验主义的演进逻辑。[40]坚持包容审慎理念，有利于促进发展与安全、公平和效率、自律和他律的动态平衡，最大限度地鼓励和支持创新，赋能科技产业发展。

3.敏捷治理

敏捷治理是面向动态发展的产业，统筹发展和安全的一条路径，是建设动态机制提升治理能力的一种理念。敏捷的理念一定程度上借鉴自 20 世纪 90 年代软件工程领域的“敏捷开发”[41]。2018 年，世界经济论坛对第四次工业革命中的政策制定问题进行反思，正式提出了“敏捷治理”（Agile Governance），将其界定为具有适应性、以人为本、包容性和可持续性的政策制定，并且要引导越来越多的利益攸关方积极参与。与会代表认为这是快速驾驭变化、主动或被动地拥抱变化并从变化中学习的持续准备，同时为实际或设想的最终用户价值作出贡献。[42]2022 年，中共中央办公厅、国务院办公厅印发《关于加强科技伦理治理的意见》，将敏捷治理列为五大治理要求之一，强调“加强科技伦理风险预警与跟踪研判，及时动态调整治理方式和伦理规范，快速、灵活应对科技创新带来的伦理挑战”。《全球人工智能治理倡议》等文件中也都强调了敏捷治理。此前，2019 年，中国国家新一代人工智能治理专业委员会发布《新一代人工智能治理原则——发展负责任的人工智能》，将敏捷治理列为八项原则之一，并进行了具体阐释；在其 2021 年发布的

《新一代人工智能伦理规范》中，也在管理规范部分规定了“推动敏捷治理”。可见，敏捷治理已经成为我国人工智能治理中的一项基本理念和原则。其核心意义在于，强调尊重人工智能发展规律并保持跟踪研判，强调治理节奏上的快速回应和尽早介入，治理规则上推进弹性原则与具体类型化规则有效结合，治理关系上的互动合作以及治理方式上的过程快、力度轻的引导性治理。[43]

敏捷治理是针对发展迅速、影响广泛的新领域提出的一种治理范式。人工智能的科技发展和产业应用高速迭代，要求在研发和应用过程中，根据发展变化或新的信息来及时调整治理策略和措施，以保障人工智能的安全、可靠和可控。敏捷治理特别强调前瞻性的视野和方法，尤其是努力尝试在问题出现之前对问题的预测研判。[44]在这个意义上，敏捷治理也是一种“预防性法治”。[45]因此，敏捷治理要求建立稳定良好的信息获取能力和机制，保障面对不确定性问题时能够及时获取广泛、多样、充分的意见，[46]要求建立健全风险沟通、风险报告和预警机制，并持续加强对风险的研究和预判能力。

4.可持续发展

以人为本和发展导向的核心理念也决定了应将可持续发展作为一项基本理念。可持续发展强调在推进技术发展的同时，确保这种发展促进经济、社会和环境的长期健康和平衡，包括环境友好（绿色发展）、节约资源、减少不平等和数字鸿沟、促进教育和就业、提高公共服务的质量和可及性、尊重和保护文化多样性、鼓励技术开放和共享、支持全球合作等。人工智能科技自身也需要注重可持续发展，理性对待创新和投资，对过往的两次“人工智能严冬”应引以为戒。人工智能治理的可持续发展理念正在成为全球共识。联合国教科文组织发布的《人工智能伦理问题建议书》建议各国政府和机构应充分考虑到人工智能技术对于联合国可持续发展目标的影响。[47]我国发布的《全球人工智能治理倡议》也提出，积极支持以人工智能助力可持续发展，应对气候变化、生物多样性保护等全球性挑战。这些都应成为人工智能治理应坚持的基本理念、价值标准和行动准则，从而赋能社会公众平等受益于人工智能的发展，并赋能我国深度参与全球人工智能治理体系建设。

四、赋能型人工智能治理的机制构建

在人工智能治理机制设计中，应自觉将“赋能”作为重要目标，将前述核心和基本理念融入人工智能治理相关的各方面机制设计之中。赋能型人工智能治理的具体机制仍需不断研究发展。当前在整体上应建设以法治为核心的人工智能治理机制，并聚焦关键问题，建设法治统领下的各项具体机制。

（一）构建以法治为核心的赋能型人工智能治理机制

之所以要构建以法治为核心的人工智能治理机制和体系，从原理而言，是因为“法治是治国理政的基本方式”[48]，“是现代社会治理的基本手段”[49]，“依法治理是最可靠、最稳定的治理”[50]，“是中国式现代化的重要保障”[51]，是贯彻以人为本和发展导向的核心理念、赋能人工智能安全可信发展的关键支撑。

第一，从“软法”治理到以“硬法”为引导和保障、“软法”与“硬法”相结合的治理形态，是人工智能治理的必然趋势。过去人工智能大国的人工智能治理主要依靠“软法”，即依人工智能科技伦理、行业规范和技术标准等，但是，随着人工智能发展特别是人工智能大模型这类颠覆性技术的安全风险的外溢，“软法”的局限性和低效能日益显现，并且难以给予企业明确预期。于是，人工智能治理正在由“软法”治理转向以“硬法”为引导和保障、“软法”与“硬法”协同治理的新形态。这标志着人工智能治理在法治轨道上有序推进。

以“硬法”为引导和保障不代表忽视“软法”的优点和作用，而是在充分发挥“软法”的积极作用的同时，关注“硬法”可以对“软法”起到的支撑作用。在人工智能治理体系中，科技伦理、道德规范、行业规范、技术标准、企业规章、国际宣言等“软法”有其不可替代的积极作用，特别是在具体应用场景的科技伦理、行业规范和技术标准独具

指导和规范作用。“硬法”对“软法”的引领和制度性支撑可以使其更好发挥作用，以形成“内外结合、法德共治”的局面。

当前，国际上已开始重视人工智能治理的法治化和规范化。例如，欧盟陆续通过了数字领域的一系列重要法律，并在 2019 年发布的《可信人工智能伦理指南》的基础上，制定和通过了《人工智能法》。这标志着欧盟在人工智能治理中从“软法”到“硬法”的转变升级。美国则出台了系列行政命令，如《关于安全、可靠和值得信赖地开发和使用人工智能的行政命令》等，对行政部门等作出了明确工作部署和要求。[52]

我国人工智能治理的“硬法”保障还滞后于人工智能发展和安全保障的需求。尽管我国已经制定实施了《网络安全法》《数据安全法》《个人信息保护法》等与人工智能相关的法律及行政法规、地方性法规，出台了《生成式人工智能服务管理暂行办法》等多部相关部门规章，但还缺少专门的人工智能法律和行政法规，尤其是缺少一部人工智能基本法。2017 年国务院印发的《新一代人工智能发展规划》提出，“到 2025 年初步建立人工智能法律法规，到 2030 年建成更加完善的人工智能法律法规”。为推进这项立法规划的实施，应当在坚持科学立法、民主立法、依法立法原则和确保立法质量的基础上，加快立法步伐，把“小快灵”和“大部头”立法结合起来，经过五年左右时间形成人工智能法律法规体系，打造有利于人工智能安全可信发展的法治环境。

第二，法治是推进人工智能领域善治的必由之路。人工智能治理需要落实以人为本、发展导向的核心理念，使人工智能领域既规范有序又充满活力。达到此目标，就是我们期待的“善治”。法治正是通向善治的必由之路。法治能够将必要的规范和有效的治理机制予以确立，以法律的确定性消解人工智能的许多不确定性，使人工智能研发、提供、部署主体可以对自身活动及其结果产生稳定预期，保障和促进企业依法依规经营、人工智能科技向善发展、公民个人依法使用、社会治理能力提升，进而消减不确定因素及关联问题的发生，增强社会对于发展和应用人工智能的信心。

第三，法治是营造人工智能创新发展环境的必然要求。习近平总书记指出，“法治是最好的营商环境”[53]。根据这一科学判断，可以认为法治是人工智能最好的发展环境。其一，法治以其“权利本位”的价值导向，为人工智能领域的产权等权益保护建构法治体系，激发社会创新活力，提升自主创新能力。其二，维护公平竞争的法治秩序可以“激发市场主体发展活力，使一切有利于社会生产力发展的力量源泉充分涌流”[54]。其三，法治实施分级分类监管，对于少量的高风险人工智能采取审慎的监管，对大量风险较小的人工智能应用提供尽可能宽阔的创新空间。其四，法治为人工智能发展创造了安全的政治环境、稳定的社会环境、公正的法治环境、优质的服务环境。

（二）完善法律治理与技术治理相统合的机制

科技与法治的有机融合是人工智能治理的必由之路，是人工智能时代治理能力建设的重点。自互联网和数字技术诞生以来，以莱斯格为代表的研究者们就开始探讨数字科技与法律的关系，推进数字科技与法律的良性互动。[55]推进“符合伦理的设计”（ethically aligned design）、“通过设计保障伦理”（ethics by design）、“通过设计保护隐私”（privacy by design）等被认为是治理数字科技的重点路径。布朗斯沃德提出了“法律 3.0”的概念，强调利用技术性方案来实现政策目标，即监管机构应当自己采用（或让他人采用）技术管理措施，将规范性观点转化为实际的设计。[56]在立法和法律适用中应当充分考察科技发展情况，促进智能科技向善发展，推动关键要素和治理技术的普惠可及，并用科技赋能企业自治和政府监管，使整个社会更加高效、可控地迎接人工智能时代到来。针对当前的人工智能发展和治理现状，完善法律治理与技术治理相统合的机制，有两方面重要工作：

首先，从坚持发展导向、统筹安全发展的核心理念出发，需要在法治建设中深度研判科技发展的制度需求，赋能企业创新发展。技术治理能力的提

升本身需要以人工智能科技发展为基础。这要求法治建设切实把握人工智能科技的发展要素、发展阶段和发展需要，探求其中的关键性生产要素及其是否存在供给不充分、市场失灵等情况，对相关法律进行系统性解释或完善，合理促进关键性要素的提供和利用效率。目前对于人工智能企业而言，科技要素赋能主要是算法、算力、数据的赋能。这些要素的供给和流通利用的不充分、不公平，可能影响人工智能创新特别是中小企业的公平竞争，数据的可及性和质量问题还会影响人工智能系统的公平性、包容性、准确性、安全性等。需要建立科学有效的法律制度，促进要素质量提升、普惠可及，赋能人工智能科技和产业发展。

其次，从智能向善的理念出发，需要通过法治来促进企业不断提升人工智能技术的安全可信性，推动合规技术和监管技术的创新，赋能企业自身治理和政府监管。一方面，应当将研发、采取必要技术措施与企业注意义务相衔接，激励相应技术的发展；另一方面，还应注重不断分析梳理治理科技和管理措施相关信息，重视规则的“精确度”，[57]将抽象、弹性的法律规则与明确、具体的标准、行动指南等相结合。这些指南和标准建设也要重视法律、行政规制和技术方案之间的融贯性，[58]避免技术标准对于法律的误读。

（三）发展多元主体沟通协作的共治机制

有效、及时的多元主体沟通协作是实现包容审慎、敏捷治理理念，提升风险识别和防控能力的必然要求。风险信息和治理信息的有效交流和共享是社会治理的重要机制。人工智能的风险治理需要建立更加及时有效的沟通机制。我国近年来在新闻推荐、平台劳动算法等领域，都出现了基于社会监督以及监管机构的沟通，推动了智能算法改进的实例。未来应将人工智能风险信息和治理信息沟通进一步前置化、制度化、常态化。

首先，针对目前跨领域主体缺少信息沟通、治理对话困难等问题，需要建立由监管机构主导，人工智能企业、科研人员、行业组织、新闻媒体、社会公众等多元主体参与的制度化、常态化的风险沟通机制。参与主体的专业领域应当涵盖人工智能科技、伦理学、法学、经济学、管理学、社会学、新闻传播学、教育学、心理学等，持续建设和发布有益信息，提高透明度，完善用户及社会公众的便捷反馈渠道和处理流程，推动建设及时、便捷的风险报告和应急处理机制，建立健全立法后的法治效果评估机制。

其次，应当创新拓展试验性监管机制。建立监管沙箱是一种典型方式。在可能具有高风险的人工智能新技术新应用进入市场之前，可建立影响可控的监管沙箱，由相应的监管机构入场观察、沟通和指导，帮助创新者更好地理解合规要求、建立有效控制风险的机制，并将产品安全推向市场。我国市场监管总局、工信部等五部门联合发布的《关于试行汽车安全沙盒监管制度的通告》（2022年第6号）指出，汽车安全监管具有提高应急处置能力、防范和化解重大风险、保护消费者合法权益、鼓励企业技术创新、倡导最佳安全设计实践等重要意义。在试验性监管中，可以充分开展监管方式的创新和实验，综合运用适当的监管科技，开展人工智能社会治理实验，对风险情况进行深入评估，并探索出科学有效的风险防治措施。

最后，应当加快构建人工智能治理和能力建设的国际合作机制，为人工智能安全可信发展提供国际协作和规则保障。一方面在国内立法中明确树立我国的人工智能治理理念，明确我国开展人工智能能力建设的对外援助，增强发展中国家的自主可持续发展能力，推动国际发展合作，坚持尊重他国主权；另一方面，积极推动形成具有广泛共识的人工智能国际治理框架，建立人工智能重要风险信息的国际流通共享机制和跨国风险防控的协作机制。

（四）建立与人工智能发展相适配的避风港机制

在互联网发展过程中，避风港规则在保障互联网创新发展、促进社会合作治理等方面发挥了重要作用。在人工智能发展应用初期，赋能企业创新发展，要求法律尊重科技发展规律，明确建立与发展

阶段、具体情况相匹配的“避风港”机制和具体规则。

从数据层面看，数据利用对于人工智能产业发展极其重要。有学者指出，我国数据流通交易所需要的主要制度增量在于建立合理的数据交易相关行为法律后果的责任规则，例如，确立在数据交易所进行的满足条件的场内数据交易的避风港规则等。[59]

从算法模型及社会应用层面看，当前主流的基于机器学习的人工智能技术建立在概率的基础之上，存在一定的偏差、错误在所难免。但人工智能的错误在不同应用领域可能引起的风险的类型、程度不同，且人工智能及风险防治措施都仍在动态发展之中。因此，为人工智能产业建立分级分类的、合理的避风港规则，对于稳定产业预期、促进创新投入、推动企业采取合理措施都具有积极意义。而背离人工智能发展客观规律、实行过度严格的规制将会形成对创新的抑制作用，也会影响到社会中的人工智能安全能力建设。当然，过于宽松的责任豁免规则，也可能难以推动人工智能企业自身的“智能向善”实践。因此在建立避风港规则时要结合多元主体的沟通协作机制，建立与技术发展水平相匹配的注意义务，做到宽严适度。

（五）创建敏捷互动、激励向善发展的动态监管机制

人工智能处于高速发展阶段，为了建设有效的监管能力，可在包容审慎、敏捷治理的理念下，创建分级分类、敏捷互动、激励人工智能向善发展的动态监管机制。艾尔斯和布雷思韦特在回应型规制中提出“执法金字塔”模型，将监管工具划分为干预力度由弱至强的不同层次，并建议监管机构优先采取轻力度的干预模式，根据被监管对象的具体情况进行调整。[60]人工智能治理可以扩展这一模型，构建风险管理金字塔、监管惩戒金字塔和价值对齐激励金字塔，并基于实践中的动态信息，在风险管理要求、惩戒措施和价值对齐激励措施的不同层级间进行动态调整。

其一，建立科学分级分类、支持动态调整的风险管理金字塔。在人工智能治理实践中，金字塔模型的思路首先可以转化为分级分类的风险管理要求，即要求采取的人工智能风险管理措施应当与风险级别和类别相适配，以确保对高风险人工智能系统采取有针对性、实效性的管理措施，并为大量风险微小的人工智能应用减轻负担。

风险管理金字塔模型已经投映在许多国家和地区的法律法规、公共政策之中。欧盟《人工智能法》将人工智能系统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四个等级，并将通用人工智能模型划分为一般模型和具有系统性风险的模型两个等级，分级分类地规定了不同要求。我国相关法律法规和部门规章也体现了分级分类进行风险管理要求的立法思路。[61]例如，《互联网信息服务算法推荐管理规定》第 23 条明确规定对算法推荐服务提供者实施分级分类管理，并延续到对深度合成、生成式人工智能的管理模式。2021 年 1 月，全国信息安全标准化技术委员会发布《网络安全标准实践指南——人工智能伦理安全风险防范指引》，对人工智能伦理安全风险进行了分类，包括“失控性风险”“社会性风险”“侵权性风险”“歧视性风险”“责任性风险”，虽然该指引没有对风险等级进行划分，但从其分类术语中可以大体理解其风险级别。我国学者在人工智能立法建议中也提出了将人工智能系统基于其风险程度或关键程度，建立相对应的管理规范和监管措施。[62]

在建立分级分类管理基本框架的基础上，特别要注意人工智能仍处于高速发展阶段，关于风险和有效治理措施的信息都不充分，应当结合前述多元主体共治机制及时获取信息，并设置依法基于风险评估情况进行风险级别敏捷调整的机制，同时为企业提供风险管理措施指引，并留有合理的建设时间。

其二，建立渐进适用的监管惩戒金字塔。我国《网络安全法》《数据安全法》《个人信息保护法》等法律中都建立了从责令整改、给予警告，到没收违法所得、处以罚款、责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，以及

构成犯罪的，依法追究刑事责任等不同强度的规制措施。[63]延续此模式，人工智能领域可以建立惩戒强度逐层递进的监管惩戒金字塔，根据具体风险项的情况，结合渐进适用策略，采取合乎比例的、轻量级干预优先的惩戒措施。

其三，建立有效互动的价值对齐激励金字塔。人工智能治理体系中还应构建与企业推动智能向善实践相关联的“价值对齐激励金字塔”，以法治机制激励企业积极开展与社会价值对齐的人工智能技术研发，不断提升人工智能的安全性、准确性、稳健性、可解释性、公平性、包容性、隐私保护等重要指标，进而提升企业和整个社会在人工智能时代的安全可信保障能力。对于积极创新发展与社会价值对齐的人工智能技术的企业，可以采取给予行政奖励、进行信用联合激励、给予信用优惠或税收优惠等激励制度。[64]以此弥补传统监管机制中对于支撑人工智能价值对齐、安全可信的技术研发投入激励不足的情况，切实促进智能向善。

（六）建设人工智能保险等社会保障机制

社会保障能力和机制建设是赋能型人工智能治理的重要方面。保险制度是现代风险治理中的一种重要工具，不但可以在灾害之后进行补偿，还可以发挥事先降低与管控风险的作用。首先，保险具有敏捷调整性。特别是面对新型技术，相比侵权责任体系，保险能够更快速地收集数据和进行评估，并且能够更加敏捷灵活地根据新技术及其安全措施的发展情况来持续进行更新和调整。[65]其次，在新技术发展早期，法律通常需要为发展留有必要的空间，如为人工智能明确设置避风港规则，此时保险可以填补侵权法留下的空白，为利益受损者提供金钱救济。[66]最后，保险可以通过设置保险范围限制和例外、进行保险核保并提供信息、调整保费等一系列措施来发出信号，激励和引导相关主体调整其行为，例如，采取更有效的风险管理措施，从而减轻与人工智能新兴技术相关的风险，同时为人工智能公司和人工智能用户提供更多的安全保障。这将允许不同的利益相关者继续释放人工智能的力量及其对社会的价值。[67]

从国际上来看，科技界和法学界对为机器人、自动驾驶等高风险人工智能产品建立保险制度的问题讨论了多年。我国一些地方出台的有关自动驾驶的地方性法规或规章中也明确规定了强制性的购买保险要求。[68]同时，我国也在积极探索网络安全保险制度，[69]这既可以为人工智能系统的网络和数据安全风险的保障提供保险机制，也可为更专门化的人工智能保险提供参考。

可以看到，人工智能系统的保险制度在实践中已经得到了一定程度的重视，但具体保险制度建构方案不尽相同，并且存在道德风险、缺少全球性指南、购买主体存在争议、保费估计困难等很多问题。[70]为实现有效赋能可信发展的目标，应进一步研究探索合适的人工智能保险制度构建方案。可以率先在自动驾驶等高风险人工智能领域开展试点，通过保险制度稳步推动人工智能安全评估、监测、应急处理、救济等能力建设，增强人工智能社会治理能力。

同时，需要推进与人工智能相关的通识义务教育、职业技能培训、就业促进机制等民生保障建设，消除数字鸿沟，赋能社会公众在人工智能发展中平等获益，也为人工智能科技的社会监督、科学运用奠定良好的基础。

五、结语

人类社会正在快速进入以新一代人工智能为标志的智能时代。人工智能有望赋能千行百业，但当前其自身发展也需要治理赋能。人工智能所处的发展阶段、人工智能发展的机遇和挑战、人工智能风险的基本特征、人工智能治理能力的现存缺陷、既往规制模式的局限性等，都共同指向“赋能型人工智能治理”。如何营造有利于人工智能创新发展的良好法治环境和人文环境，保障人工智能技术科学研发、安全运用、向善发展，增强人工智能企业的合理预期，增强监管能力，增强社会对于人工智能应用的信任，进而有效推动人工智能安全可信发展，是亟待回答的重要问题。应通过依法有效治理来赋能人工智能安全可信发展，并最终赋能社会、

赋能人民。我们需要确立赋能型人工智能治理新理念，健全以法治为核心的赋能型人工智能治理新机制，迈向赋能型人工智能治理新格局，将科技发展与国家治理体系和治理能力现代化有机结合，服务于数字中国建设和中国式现代化进程，并为全球人工智能治理作出贡献。

参考文献

[1]《中共中央关于进一步全面深化改革 推进中国式现代化的决定》，2024 年 7 月 18 日中国共产党第二十届中央委员会第三次全体会议通过。

[2] 参见《联大通过中国提出的加强人工智能能力建设国际合作决议》，载中国政府网，https://www.gov.cn/yaowen/liebiao/202407/content_6960524.htm，2024 年 7 月 2 日访问。

[3] 参见李强：《政府工作报告》，2024 年 3 月 5 日在第十四届全国人民代表大会第二次会议上。

[4] 参见［英］安东尼·吉登斯：《现代性的后果》，田禾译，译林出版社 2022 年版，第 39、93、102 页。

[5] See Ronald Leenes, Regulating New Technologies in Times of Change, in Leonie Reins ed., Regulating New Technologies in Uncertain Times, ASSER Press, 2019, p.8-9.

[6] 黄先海、宋学印：《赋能型政府——新一代政府和市场关系的理论建构》，载《管理世界》2021 年第 11 期，第 47-48 页。

[7] See Regulation of the European Parliament and of the Council of Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), at https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/en/pdf (Last visited on May 25, 2024).

[8] See Jason Wei et al., Emergent Abilities of Large Language Models, Transactions on Machine Learning Research, No.8, p.11 (2022).

[9] See Stanford Institute for Human-Centered Artificial Intelligence, Artificial Intelligence Index Report 2024, p.30, at https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf (Last visited on March 15, 2024).

[10] See Robert P. Merges, Uncertainty and the Standard of Patent ability, High Technology Law Journal, Vol.7, p.20-25 (1992).

[11] 参见中国行政管理学会课题组：《聚焦市场主体关切 持续打造市场化法治化国际化营商环境》，载《中国行政管理》2021 年第 8 期，第 6 页。

[12] 参见习近平：《在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话》（2018 年 5 月 28 日），人民出版社 2018 年版，第 13 页。

[13] 参见丁晓东：《论人工智能促进型的数据制度》，载《中国法律评论》2023 年第 6 期，第 175-191 页。

[14] 参见严驰：《论人工智能的激励型立法——基于〈拜杜法〉的思考》，载《人工智能》2024 年第 2 期，第 95-96 页。

[15] 参见苏宇：《算法规制的谱系》，载《中国法学》2020 年第 3 期，第 167-169 页。

[16] 参见苏宇：《大型语言模型的法律风险与治理路径》，载《法律科学》2024 年第 1 期；刘金瑞：《生成式人工智能大模型的新型风险与规制框架》，载《行政法学研究》2024 年第 2 期。

[17] See Peter Huber, Safety and the Second Best: The Hazards of Public Risk Management in the Courts, Columbia Law Review, Vol.85(2), p.277 (1985).

[18] 参见［英］安东尼·吉登斯：《第三条道路——社会民主主义的复兴》，郑戈译，北京大学出版社 2000 年版，第 65-66 页。

[19] See Rebecca B. Naumann, et al., Examining the Safety Benefits of Partial Vehicle Automation Technologies in an Uncertain Future, Technical Report, AAA Foundation for Traffic Safety, 2023, p.39.

[20] 参见赵鹏：《风险社会的行政法回应》，中国政法大学出版社 2018 年版，第 77 页。

[21] 参见［德］乌尔里希·贝克、［德］约翰内斯·威尔姆斯：《自由与资本主义——与著名社会学家乌尔里希·贝克对话》，路国林译，浙江人民出版社 2001 年版，第 121 页。

[22] 参见前注[4]，安东尼·吉登斯书，第 44 页。

[23] 前注[18]，安东尼·吉登斯书，第 67 页。

[24] 参见卢超：《包容审慎监管的行政法理与中国实践》，载《中外法学》2024 年第 1 期，第 159 页。

[25] See Cary Coglianese, Engaging Business in the Regulation of Nanotechnology, in Christopher J. Bosso ed., Governing Uncertainty: Environmental Regulation in the Age of Nanotechnology, Resources for the Future Press, 2010, p.49-51; ［英］罗伯特·鲍德温、［英］马丁·凯夫、［英］马丁·洛奇：《牛津规制手册》，宋华琳等译，上海三联书店 2017 年版，第 165-166 页。

[26] See Bridget M. Hutter, Regulating Employers and Employees: Health and Safety in the Workplace, Journal of Law and Society, Vol.20(4), p.452-470 (1993); Keith Hawkins, Environment and Enforcement: Regulation and the Social Definition of Pollution, Oxford University Press, 1984, p.4.

[27] See Thomas Ferretti, An Institutionalist Approach to AI Ethics: Justifying the Priority of Government Regulation over SelfRegulation, Moral Philosophy and Politics, Vol.9(2), p.244-256 (2022).

[28] 科林格里奇困境（Collingridge's Dilemma）是英国技术哲学家大卫·科林格里奇在《技术的社会控制》中提出的“控制困境”，即试图控制一项技术是非常困难的，因为在技术发展早期还可控时，对其有害的社会后果认知不足，难以证明控制其发展的必要性；但当有害社会后果已经很明显了，控制亦已昂贵而缓慢。See David Collingridge, The Social
Control of Technology, Frances Pinter, 1980, p.19.

[29] See Ian Ayres & John Braithwaite, Responsive Regulation: Transcending the Deregulation Debate, Oxford University Press, 1992, p.35-37; Neil Gunningham, Enforcement and Compliance Strategies, in Robert Baldwin, Martin Cave & Martin Lodge eds., The Oxford Handbook of Regulation, Oxford University Press, 2010, p.125-131.

[30] See Ian Ayres & John Braithwaite, supra note 29, 38-39.

[31] 参见前注[25]，罗伯特·鲍德温等书，第 168-170 页。

[32] 参见黄文艺、孙喆玥：《论互联网平台治理的元规制进路》，载《法学评论》2024 年第 4 期，第 112 页。

[33] 参见张凌寒：《平台“穿透式监管”的理据及限度》，载《法律科学》2022 年第 1 期，第 107 页；张欣：《生成式人工智能的算法治理挑战与治理型监管》，载《现代法学》2023 年第 3 期，第 117 页；郭小东：《生成式人工智能的风险及其包容性法律治理》，载《北京理工大学学报（社会科学版）》2023 年第 6 期，第 93 页。

[34] Asilomar AI Principles, at https://futureoflife.org/open-letter/ai-principles/ (Last visited on March 15, 2024).

[35] 参见许为、葛列众、高在峰：《人—AI 交互：实现“以人为中心 AI”理念的跨学科新领域》，载《智能系统学报》2021 年第 4 期，第 613 页。

[36] 参见前注[1]，《中共中央关于进一步全面深化改革 推进中国式现代化的决定》。

[37] 习近平：《决胜全面建成小康社会 夺取新时代中国特色社会主义伟大胜利——在中国共产党第十九次全国代表大会上的报告》（2017 年 10 月 18 日），人民出版社 2017 年版，第 21 页。

[38] 即在没有约束或引导的情况下，企业的研发力量往往大量投入于与企业未来盈利具有明显关系的领域，对弱势群体权益保障、数字无障碍技术、安保技术等往往投入不足。

[39] 参见《李强在北京调研时强调 推进科技创新和产业创新深度融合 加快塑造高质量发展新动能新优势》，载《人民日报》2024 年 3 月 14 日，第 1 版。

[40] 参见前注[24]，卢超文，第 143 页。

[41] Torgeir Dingsøyr et al., A Decade of Agile Methodologies: Towards Explaining Agile Software Development, Journal of Systems and Software, Vol.85:1213, p.1213-1221 (2012).

[42] See World Economic Forum, Agile Governance: Reimagining Policy-making in the Fourth Industrial Revolution, White Paper, Jan. 2018, p.4, at https://www3.weforum.org/docs/WEF_Agile_Governance_Reimagining_Policy-making_4IR_report.pdf (Last visited on March 15, 2024).

[43] 参见薛澜、赵静：《走向敏捷治理：新兴产业发展与监管模式探究》，载《中国行政管理》2019 年第 8 期，第 31-33 页；赵静、薛澜、吴冠生：《敏捷思维引领城市治理转型：对多城市治理实践的分析》，载《中国行政管理》2021 年第 8 期，第 52-53 页。

[44] See Helmut Anheier & Edward Knudsen, Agile Governance, at https://intelligence.weforum.org/topics/a1Gb0000000pTDaEAM (Last visited on March 15, 2024).

[45] 参见黄文艺：《论预防型法治》，载《法学研究》2024 年第 2 期，第 20-38 页。

[46] See Agile Governance: Managing Uncertainty, at https://intelligence.weforum.org/topics/a1Gb0000000pTDaEAM/keyissues/a1G680000004CtBEAU (Last visited on March 15, 2024).

[47] 参见联合国教科文组织：《人工智能伦理问题建议书》，载联合国教科文组织官网，https://unesdoc.unesco.org/ark:/48223/pf0000380455_chi，2024 年 3 月 15 日访问。

[48] 习近平：《关于〈中共中央关于全面推进依法治国若干重大问题的决定〉的说明》（2014 年 10 月 20 日），载习近平：《论坚持全面依法治国》，中央文献出版社 2020 年版，第 84 页。

[49] 习近平：《坚持法治精神，实现公平正义》（2017 年 9 月 26 日），载前注[48]，习近平书，第 183 页。

[50] 习近平：《依法保障“一国两制”实践》（2014 年 11 月—2019 年 12 月），载前注[48]，习近平书，第 120-121 页。

[51] 前注[1]，《中共中央关于进一步全面深化改革推进中国式现代化的决定》。

[52] See Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthydevelopment-and-use-of-artificial-intelligence/ (Last visited on March 15, 2024).

[53] 习近平：《为做好党和国家各项工作营造良好法治环境》（2019 年 2 月 25 日），载前注[48]，习近平书，第 254 页。

[54] 习近平：《在经济社会领域专家座谈会上的讲话》（2020 年 8 月 24 日），人民出版社 2020 年版，第 7 页。

[55] See Lawrence Lessig, The Law of the Horse: What Cyberlaw might Teach, Harvard Law Review, Vol.113(2), p.514 (1999)；齐延平：《数智化社会的法律调控》，载《中国法学》2022 年第 1 期，第 79 页。

[56] 参见［英］罗杰·布朗斯沃德：《法律 3.0：规则、规制和技术》，毛海栋译，北京大学出版社

2023 年版，第 1-5 页。

[57] See Colin S. Diver, The Optimal Precision of Administrative Rules, Yale Law Journal, Vol.93, p.66 (1983).

[58] 参见郭春镇：《生成式 AI 的融贯性法律治理——以生成式预训练模型（GPT）为例》，载《现代法学》2023 年第 3 期，第 88 页。

[59] 参见戴昕：《作为法律技术的安全港规则：原理与前景》，载《法学家》2023 年第 2 期，第 43-45 页。

[60] See Ian Ayres & John Braithwaite, supra note 29, 38-39.

[61] 我国《网络安全法》《数据安全法》《个人信息保护法》等法律中都体现了风险管理金字塔模型的基本思路，包括实施网络安全等级保护制度，对重要数据、敏感个人数据加强风险管理要求等。

[62] 例如，《人工智能法示范法 2.0（专家建议稿）》实际上将人工智能风险划分为高风险、中风险、低风险三个级别，规定了不同风险管理要求和监管机制。参见周辉等：《人工智能法示范法 2.0（专家建议稿）》，载上海市人工智能社会治理协同创新中心官网，https://aisg.tongji.edu.cn/info/1005/1211.htm，2024 年 9 月 14 日访问。《中华人民共和国人工智能法（学者建议稿）》建议区分一般的人工智能系统和关键人工智能系统，对后者规定了更多要求。参见张凌寒等：《中华人民共和国人工智能法（学者建议稿）》，载北京航空航天大学法学院官网，https://fxy.buaa.edu.cn/info/1143/8452.htm，2024 年 9 月 14 日访问。

[63] 参见《网络安全法》第 59-69 条；《数据安全法》第 45 条；《个人信息保护法》第 66 条；等等。

[64] 参见喻文光：《论数字平台的合规监管》，载《法学家》2024 年第 1 期，第 126-127 页。

[65] See Kenneth S. Abraham, The Liability Century — Insurance and Tort Law from the Progressive Era to 9/11, Harvard University Press, 2008, p.1256-1266.

[66] See Jeffery L. Vagle, Cybersecurity and Moral Hazard, Stanford Technology Law Review, Vol.23(1), p.100 (2020).

[67] See Anat Lior, Insuring AI: The Role of Insurance in Artificial Intelligence Regulation, Harvard Journal of Law & Technology, Vol.35(2), p.511-519 (2022).

[68] 例如《北京市自动驾驶车辆道路测试管理实施细则（试行）》第 8 条第（五）项、《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》第 30 条。

[69] 2023 年 7 月，工信部、国家金融监督管理总局联合发布了《关于促进网络安全保险规范健康发展的意见》；2023 年 7 月，国家市场监督管理总局和国家标准化管理委员会联合发布了《信息安全技术 网络安全保险应用指南》（征求意见稿）；2023 年 12 月，工信部发布了《关于组织开展网络安全保险服务试点工作的通知》。

[70] See Anat Lior, supra note 67, 499-504; 刘艳红：《自动驾驶的风险类型与法律规制》，载《国家检察官学院学报》2024 年第 1 期，第 119 页。

论人工智能立法的基本路径

原载：《中国法学》2024 年第 5 期，第 82-102 页

作者：林洹民

摘要：采用何种路径规范人工智能活动，是人工智能立法的核心问题。风险管理进路存在风险评估与分类困难、放任损害发生等问题，并非人工智能立法的当然选择。与以往科技活动不同，人工智能活动既属于专精科技活动，又具有赋能科技活动属性。以人工智能活动为规范对象的人工智能法不应以单一理论为指导，而应遵从科技法与应用法双重定位。科技法定位下的《人工智能法》应尊重科技自主，将科技伦理内化于人工智能研发活动中，同时打破制度壁垒，设计促

进型规则，助力人工智能科技的发展。应用法定位下的《人工智能法》则应关注科技赋能场景导致的功能异化现象，一方面借助抽象的权利义务工具，尤其是通过规定新型权利，构建弹性的规范框架，回应不同应用场景中的价值序列差异；另一方面应推行实验主义治理，通过监管沙箱、授权性立法等设计，动态调整监管策略，满足人工智能赋能应用活动的灵活治理需求。

一、引言

随着人工智能技术的发展与应用，人工智能治理正在引起国际社会的高度重视。立法机构已经不满足于伦理宣言式的行业自治，转向出台专门性的法律，从而开启了从“软拘束”到“硬规则”的人工智能立法时代。欧盟于 2021 年率先推出全面规范人工智能活动的法律《人工智能法（提案）》（The Artificial Intelligence Act）。该提案经过修正后，于 2024 年 3 月经欧洲议会表决通过，这标志着欧盟诞生了世界上首部规范人工智能活动的综合性法律。美国在联邦层面尚没有进行类似的横向集中式立法，但也于 2023 年 10 月发布“具有里程碑意义的”总统行政命令，要求美国联邦政府各部门和机构制定人工智能活动监管政策。在我国，国务院自 2023 年开始已经连续两年将人工智能立法列入立法工作计划；全国人大常委会于 2023 年 9 月发布的《第十四届全国人大常委会立法规划》也将人工智能立法列入第一类项目（条件比较成熟、任期内拟提请审议的法律草案），并指出“推进科技创新和人工智能健康发展……要求制定、修改、废止、解释相关法律，或者需要由全国人大及其常委会作出相关决定的，适时安排审议”。可以预见，一旦完成准备工作，我国人工智能立法将会提速进行。

围绕人工智能立法的争议问题包括但不限于以下五点：人工智能法的规范对象、人工智能立法的基本路径、人工智能时代的新兴权利、监管机构以及法律责任。其中，对人工智能活动的规范进路问题涉及价值判断与治理观念，反映了立法者应对未知的伦理观。就立法基本路径而言，极端谨慎的态度是，如果不能防范风险，就不允许新技术的应用，但这一方案明显过于保守。与之相对，风险管理进路强调拥抱风险、容忍错误，对技术研发与应用更为友善。欧盟的《人工智能法》就明确采取风险管理进路规范人工智能活动，该法“序言”第 14 条指出，法案遵循“基于风险的路径”（risk-based approach），即根据人工智能系统可能产生的风险的强度和范围来确定规则的类型和内容。在英国达成的全球第一份针对人工智能的国际性声明《布莱切利宣言》，同样强调应采取“基于风险的政策”调整人工智能活动。我国也签署了《布莱切利宣言》，接受基于风险的人工智能规范路径。然而，风险管理进路未必合理。笔者认为，我国如果简单地照搬他国模式进行人工智能立法，不仅无法为世界法治贡献智慧成果，也将丧失引领人工智能全球治理的良机。是以，研究人工智能立法的基本路径问题，既是发展我国本土法学、树立中国法学界碑的应有之义，也是开展人工智能国际合作、贡献中国智慧、表现大国担当的当然之举。

有鉴于此，本文将在分析风险管理进路利弊的基础上，通过辨析人工智能活动的双重属性，提出人工智能立法的另一种思路与策略，努力打造一种既能满足人工智能动态监管需求，又能促进人工智能创新发展的新型治理框架。

二、人工智能立法风险管理单一进路之检讨

或许是受到“风险社会”理论的影响，人们往往下意识地选择风险管理路径调整新兴科技活动。但风险管理进路不同于风险社会理论，后者是探讨后现代社会家庭、职业、知识以及外部自然环境等因素的风险特征的理论体系，前者则是一套基于“风险—收益”分析的社会管理方法。风险管理进路的模式是：首先，将损害界定为风险；其次，评估可能引发风险的行为；最后，在进行成本收益分析的基础上划分特定的风险分类并配置相应的规范。风险管理进路通过评估风险的危害程度、控制风险的成本以及风险能带来的收益，选择相应的规

范设计。[1]其中，将损害视为风险是风险管理的正当性基础，风险评估是风险管理的前提，而风险分类则是风险管理的关键。然而，未经充分论证就将损害界定为风险，有轻视个人权益保护之嫌；由于人工智能活动引发的风险具有高度复杂性，对人工智能活动的风险评估与分类也极为困难，风险管理路径未必能有效地调整人工智能活动。

（一）风险管理的正当性问题

正当性问题是人工智能风险管理进路受到批评的重要原因。风险管理进路强调拥抱风险、容忍错误，对技术研发与应用极为友善。但是，包容审慎的治理思路以不严重侵犯个人权益和产生重大社会风险为前提。[2]欲在政策上选择风险管理进路，必须首先论证为什么让个体与社会承受不可知的重大损害是值得的。易言之，既然已经确定地知道人工智能将产生风险，且风险可能会造成严重的损害，为什么要选择一种容忍损害的规范路径？

一种辩护观认为，风险与收益同在，个体虽然承受损害，但也在享受技术发展带来的红利。例如，智能手机极大地提升了人们的生活质量，大部分人已经无法在没有智能手机陪伴下生活。但是，并非所有人都是科技的受益者。在科技转化过程中存在决策者、受益者与波及者三方主体。波及者是不能参与政策制定又难以享受科技福利的群体。在风险管理路径下，偏离一般基准的人，如老人、低智力群体，往往被迫承受技术发展的不利后果，他们的特别需求也常被忽视。[3]另有观点认为，为了集体或多数人的利益，有时不得不让少数人承受损失。集体利益确实常被视为承受风险的理由，[4]相较于个人，群体和社会才是风险管理进路关注的重点[5]。但个人利益与集体利益是难以划分的，当海量个体沦为人工智能客体时，集体利益也在被侵犯。因而，风险管理进路未必对整体有益。

值得庆幸的是，人们已逐渐认识到风险管理路径的弊端，转而考虑采用其他替代策略。例如，在环境保护方面，德国环境保护法就抛弃之前的风险管理模式，转采预防原则。预防原则的宗旨是，面对科学上的不确定性，政策制定者应努力防止危害的发生。即便缺少损害与行为之间充分的因果关系论证，只要损害后果可能极为严重，政府也应马上采取监管措施。目前，预防原则已被写入众多环境保护公约中，取代风险原则成为环境保护的基本原则。[6]在人工智能治理领域，业界也有要求强化对人工智能活动监管，对特定人工智能活动适用许可制度而非风险管理的呼声。[7]除此之外，还有美国学者针对人工智能损害的不可逆性，强调应努力构建某种恢复性制度（Resilience），以替代人工智能风险管理模式。[8]

（二）风险评估的可行性问题

抛开正当性不论，人工智能活动风险管理进路在应用层面的可行性也存在问题。风险管理以有效的风险评估为前提。风险评估本质是一种成本效益分析，欧盟《人工智能法》第 3 条就将风险界定为发生损害的概率和该损害的严重程度的组合。风险只有被量化分析，才有可能与收益相比较，从而确定可接受的限度。但是，对人工智能活动引发风险的量化分析极为不易，人工智能风险评估未必能成为决策的基础。

其一，欠缺高质量的数据和有效的模型。首先，缺乏作为量化评估基础的高质量数据。风险评估需要的基本数据包括损害的危害程度、发生的概率、损害的地理和时间分布（普遍性）、损害的持续时间（持续性）、损害的可逆性等。[9]然而，在新技术被投入应用前，并不存在可供评估风险的相应数据。即便就已投入应用的产品而言，受技术发展、地理、时间等各方面因素影响，所提供的数据也未必具有参考性。尤其是，以 ChatGPT、Gemini 为代表的人工智能大语言模型具有强大的自我学习能力，依据既有的数据难以预测不断进化的人工智能活动带来的风险。在缺乏高质量数据的情况下，显然难以精确地计算风险发生的概率与危害程度，也就无法借助成本收益法确定人工智能活动可容忍的限度。[10]其次，目前并不存在评估人工智能风险的有效模型。对新兴技术的风险评估，将因延用旧有的分析框架而无法精确界定与测量风险。以化学材料为例，“定量结构—活性关系”（QSAR 模型）

工具可为普通化学品提供相当可靠的风险估计，但纳米材料的毒性受化学结构以外的其他因素（包括尺寸、表面积、表面特性等）影响，因而“定量结构—活性关系”并不能有效分析多数纳米材料的风险。[11]又如，目前对于机动车的检测标准与程序并不适用于智能网联汽车，《医疗器械监督管理条例》《医疗器械生产监督管理办法》也未必能够合乎预期地调整人工智能医学辅助器械（如看护机器人）的生产与使用。可见，如果使用旧有模型评估新型人工智能活动带来的风险，评估结果将不具有参考价值。当评估模型失效时，即便存在有效的数据，风险评估也将缺乏说服力。

其二，难以准确评估技术叠加引发的风险。一般技术引发的风险相对简单，风险发生概率与损害也容易确定（如机动车交通肇事风险、断电风险等）。但人工智能大语言模型引发的风险具有叠加性，使得风险评估更为困难。复杂系统中不同活动和事件之间的相互作用使得风险成倍增加，引发协同效应，风险总量远大于各部分之和。[12]有时两个或更多的故障孤立地看均不具有破坏性，可一旦故障以意想不到的方式结合在一起，就会使得安全装置失效，引发重大系统性事故。在“大模型+具体应用”的产业生态中，上游基础大模型和下游具体应用之间存在着复杂的依存关系。通过海量数据训练出的大模型为具体模型提供底层逻辑支持，具体模型则通过“术业有专攻”的专业优化训练,适配众多的具体的行业和场景。[13]在这一协同应用关系中，对上游大模型的风险评估无法预计下游应用产生的具体风险，对下游应用的风险评估也无法预测反馈机制对上游大模型自我学习能力的影响。

人工智能风险评估技术越不可靠，评估结果受到外部因素干涉的可能性就越大。近几十年来，学者们对技术风险评估的客观性进行了检验，发现偏见、道德、政策、社会文化等均会影响风险的识别与评估。[14]其中，政策对于风险评估结果的影响尤其引人关注。温迪-瓦格纳将外部政策环境对风险评估的影响评价为“科学骗局”（science charade），即用看似客观的技术评估为幌子，就技术的应用作出政策决定。[15]尤其是当人工智能活动风险评估在技术层面遭遇障碍时，风险评估就更易受到外部社会政治环境的影响。此时，财富生产的逻辑总能获胜。[16]如果风险评估变为隐性的政策选择，风险控制阀门将有失效之虞。

（三）风险分类的融贯性问题

如上所述，风险分类是风险管理的关键。风险管理路径力求将人工智能活动引发的风险进行分类，进而配置与风险级别相称的规范。目前国际上的风险分类模式主要有三种：风险属性划分模式、风险内容划分模式以及风险程度划分模式。但上述模式均存在弊端，不能融贯地划分风险的类型与级别。

1.风险属性划分模式

风险属性划分模式是一种依据风险属性对人工智能活动进行分类的治理模式。采用此种模式的典型代表为美国。美国商务部国家标准与技术研究院推出的《人工智能风险管理框架》（AIRMF1.0）根据风险属性不同，将人工智能活动风险分为技术性风险、“社会—技术”风险与指导原则性风险。技术性风险是指影响人工智能运行稳健性和准确性的风险，“社会—技术”风险涉及人工智能对隐私、安全、自由、公平等价值的影响，指导原则性风险则是人工智能的应用可能会影响对“好的”或“可信赖”的人工智能的理解。[17]这一模式的最大问题是，风险本身难以被精确定性。首先，技术一定会出错，而如何分配错误本身就是一个社会价值判断，并不存在纯粹的技术性风险。其次，“社会—技术”风险与指导原则性风险之间难以区分，因为只有在具体的应用场景中才能判断“好的”或“可信赖”。以深度伪造技术为例：当深度伪造技术被用于合成虚假图片、视频时，我们会觉得人工智能不可信赖；但当深度伪造技术被用以重现消失的艺术时，人们又乐于享受这一应用，认为人工智能是“好的”“可信赖的”。[18]对人工智能技术的宏观评价，离不开具体语境中的价值衡量。从该意义上说，指导原则性风险本质上也是一种“社会—技术”

风险。依据风险属性划分风险类型的思路，在逻辑上并不清晰，也因此欠缺可执行性。

2.风险内容划分模式

风险内容划分模式是依据风险现实化的后果进行分类。我国信息安全标准化技术委员会在 2021 年发布的《网络安全标准实践指南——人工智能伦理安全风险防范指引》依据风险后果将人工智能活动风险分为“失控性风险”“社会性风险”“侵权性风险”“歧视性风险”“责任性风险”五类；英国科技创新与技术部在 2023 年推出的《人工智能管理的创新优先路径》报告也根据风险现实化后果分类，但将人工智能风险划分为“人权风险”“安全风险”“公平风险”“隐私风险”“社会福利风险”与“可靠性风险”六类。[19]可见，即便采取同样的风险分类方式，中英两国的风险分类也并不相同。由于观察者会因信息获得渠道与关注焦点不同而总结出不同的风险类型，风险内容划分模式很难形成一套具有说服力的风险类型。更何况，列举难免会挂一漏万。立法者若依据该模式确定人工智能风险类型，可能会自我设限，使得一些本应受到充分关注的人工智能活动被排除在法律规范之外。

3.风险程度划分模式

风险程度划分模式是目前最受关注的风险分类模式。在该模式下，立法者根据人工智能活动引发风险的危害程度划分风险类型。欧盟《人工智能法》为该模式的典型代表。该法将人工智能活动引发的风险分为四类，并相应地配置规则：引发不可接受风险的人工智能系统是被禁止的，高风险人工智能系统必须遵守特定要求，限制性风险人工智能系统受到拘束较少，最小风险人工智能系统则完全不受到限制。但这一模式也存在明显的局限性。其一，风险程度缺乏明确的判断标准。例如，欧盟《人工智能法》第 7 条第 1 款要求结合“是否严重危害健康和安全”和“是否对基本权利、环境以及民主和法治造成严重不利影响”来判断人工智能活动是否属于高风险，但上述标准具有巨大的弹性与模糊性。欧盟试图通过人工智能委员会与人工智能办公室提供相对清晰的指引，但行政机关未必有能力评估风险并进行风险分类。例如，以 ChatGPT 为代表的生成式人工智能可能产生不实资讯，从而直接或间接地损害个人权益，但欧盟对于应将之归入何种类型的人工智能活动存在大量争议。[20]美国于 2024 年 5 月通过的首部规范人工智能的地方性法律《科罗拉多州人工智能法》（SB24-205），同样以高风险人工智能系统为规范对象。根据该法第 6-1-1701 条第 9 款第 a 项，构成“重大决策的实质性因素”的任何人工智能系统均为高风险人工智能系统。而这一标准可能使得所有人工智能系统都被认定具有高风险。因此，科罗拉多州不得不在该条的第 b 项规定大量例外，但也会产生“一刀切”“挂一漏万”等问题，并不能为确定是否具有高风险提供清晰的指引。其二，僵化的风险类别与高速发展的人工智能技术之间存在张力。一方面，随着人工智能技术的发展，原本被视为限制性风险或最小风险的人工智能应用可能会变得具有高风险性甚至不可接受。例如，人工智能辅助教学曾被视为教育数字化的重要标志，但随着人脸识别、情绪识别技术的发展，对学生课堂活动的监控有严重侵犯人权的风险。另一方面，原本被认为禁止应用或高风险的人工智能活动，也可能随着安全技术措施的发展与应用风险程度显著降低，但因规范的滞后性，相应的人工智能活动将受到不当限制。例如，无人驾驶引发的风险等级随着自动驾驶技术的成熟而不断降低。无人驾驶汽车越早地被投入到真实场景中进行路测，越有可能占据市场，但若无人驾驶被归入高风险人工智能活动，其路测场所、时间与程度等都将受到严格限制，最终也将制约技术发展与汽车行业的迭代升级。

风险治理作为一种现代社会治理模式，已成为“一种崇拜”，使得“一种近乎神奇的光环笼罩着对风险评估与风险治理”。[21]但若审慎地分析该模式，就会发现风险管理单一路径并非调整先进科技活动的良方。首先，风险管理路径仅适用于可量化的危害，对人工智能活动引发的风险并不适用，而忽视不可量化的危害是“灾难的根源”。[22]其次，人工智能活动的复杂性使得全面、妥当的风险分类

与归类极为困难。最后，风险管理路径有损害个体和集体利益的危险。欧盟采取风险管理进路规范人工智能活动，是一种有益的尝试，但单一理论是无法规范复杂、多场景的人工智能应用的。我国未来的人工智能立法不应受到“布鲁塞尔效应”的影响，亦步亦趋地遵循风险管理路径，而应在充分了解人工智能活动特性的基础上，寻找一种更兼顾安全与发展的综合的人工智能治理范式。

三、因应人工智能活动特性的复式立法路径

人工智能活动具有高度复杂性，以之为调整对象的法律难以按照风险管理单一路径进行设计。欲制定调整行为的法律，必须首先了解被规范的对象。如果只是基于一种主观判断进行立法，这种判断未必能够与现实问题相对应，其是否有足够的张力、体现了何种程度的偏差或遗漏，也不得而知。人工智能活动具有双重属性，人工智能立法也应具有复式立法定位。

人工智能活动由人工智能研发活动与人工智能应用活动组成，前者体现出鲜明的科学性，后者则以赋能应用为主，因此具有工具性特征。当然，人工智能研发活动与应用活动也存在交叉。例如，一些研发活动的目的是赋能应用，在应用过程中也可以通过数据训练人工智能系统，实现人工智能研发的质的突破。为了更加清晰地说明问题，下文分别着重在研发活动与应用活动的框架内讨论人工智能活动的科学性与工具性。

（一）人工智能活动的双重属性

科技大致被划分为专精科技和赋能科技两类。专精科技侧重于深度与专业性，赋能科技则注重于应用与提升能力，二者在性质、功效和实现手段上存在根本差别。以往的科技要么属于专精科技，要么表现为赋能科技。人工智能活动相较于以往的科技活动更为复杂，既具有高度专业性（科学性），又具有广泛的赋能性（工具性），同时属于专精科技活动与赋能科技活动。

1.作为专精科技活动的科学性

人工智能属于新一代科技革命中的表征性科技。人工智能研究属于一项专精科技活动，旨在开发出可以自我分析、自我总结、自我纠错的人工智能系统。为了实现这一目标，在计算机科学中产生了符号主义、联结主义和行为主义等诸多流派。[23]神经网络技术的出现使得人工智能研究有了重大突破（如深度学习算法）。以 ChatGPT 为代表的大语言模型又使得人工智能研发前进一大步。[24]目前，人工智能已经具有超强的自我学习能力。在此基础上，有些科研活动直接瞄准超级人工智能，力图使得人工智能呈现出一种人类尚未发现或无法实现的逻辑形式，进而超越人类智能，探索到人类无法触及的高度。[25]显而易见，人工智能研发本质是一项科学研究，属于专精科技活动。

人工智能研发活动的科学性增加了调整人工智能活动的难度。非专业人士通常无法真正理解作为一项科学研究的人工智能的影响。以作为人工智能三要素之一的算法为例，人工智能算法的书写甚至阅读都是一项专业技能。对非专业人士而言，算法是另外一种语言。因此，只有借助计算机科学家对科研活动的自我批判，才能理解与规范人工智能活动。目前也已经存在以控制人工智能为目标的科研项目，例如，谷歌公司、斯坦福大学等都在进行算法可视化的研究，以增强算法的可解释性。当下的研究增加了对图像识别人工智能算法的解释可能，但是仍有很多工作未能完成。[26]只有借助科学系统自身，才能更好地识别与解决问题。

2.作为赋能科技活动的工具性

当聚焦人工智能活动时，人们更多关注人工智能的赋能应用。以往的科技常被认为是定向的，影响范围基本是领域性的（如化石燃料、通信技术等），即便是通过跨学科合作产生了一定的开放性，也不具备通用性。在此认知之下，科技主要被视为推动经济发展的工具，科技法也主要关注技术的经济意义，一直秉持“技术—经济”的立法范式。[27]人工智能的出现改变了科技的定向性。人工智能是一项通用技术，是科学研究、教育、制造、物流、运输、司法、行政、广告、艺术等众多领域与人类生活各

方面的赋能者。通过在具体应用场景中的调整，人工智能可以满足多样的需求。人形机器人就是人工智能技术与场景的叠加和结合的典型。人形机器人根据不同场景需求呈现出不同的表现形式，如陪伴机器人、看护机器人以及亲密机器人等。[28]我国工业和信息化部《人形机器人创新发展指导意见》指出，应首先研发出基础版人形机器人整机，打造“公版”通用平台，然后支持不同场景需求下的结构改造、算法优化以及特定能力强化。

作为赋能工具的人工智能活动，在价值上并不当然具有合理性，可能会带来新的社会风险，导致社会关系异化。仍以人形机器人为例，在大语言模型的加持下，人形机器人将获得强大的操纵能力，损及人的主体性。其一，人形机器人具有智能表象。如果人类发现人形机器人比一般人更有能力，人形机器人迟早会获得高于普通人的影响力。[29]当我们习惯性地首先问询机器人意见时，人类就在丧失自主性。一个显而易见的例子是，高德地图、百度地图等导航程序大大减弱了个人的自主寻路能力。其二，高度拟人化的外观使得人形机器人更容易被视为“同类”。人类对于人形物件产生共情是自然的心理倾向，人形机器人的外观能够引发人类的心理投射，很容易引起共情。如果陪伴机器人或亲密机器人（性爱机器人）几可以假乱真，人类可能会有意无意地将机器人视为同类，并将之视为自己的最佳伙伴。这将使得具身智能进一步获得不同寻常的操纵能力。具有操纵性能力的人形机器人可能会限制个人的自我决定、干扰人的社会化甚至扭曲家庭观念，引发新型社会问题，因而需要法秩序积极应对与规范。[30]

（二）双重属性下的人工智能复式立法定位

基于人工智能活动的科学性与工具性双重属性，以之为规范对象的人工智能法也应具有双重定位。人工智能研发活动是一项科学研究活动，以科学活动为规范对象的《人工智能法》当然具有科技法属性；人工智能应用则是技术与场景的结合，因而以场景化应用为规范对象的《人工智能法》也应具有应用法属性。是以，我国未来的人工智能立法应同时具有科技法与应用法双重定位。

1.作为科技法的人工智能法

科技法导向下的人工智能立法应充分尊重科技自主，关注科技伦理。现代社会的典型特征是功能分化，功能分化创造解决社会问题的诸多子系统，社会子系统无法被一种方式整合，而是始终按照各自的媒介发挥作用。例如，经济子系统无法替代教育子系统的功能，科研活动也只能依托科技系统推进。[31]科研活动一般不愿受到过多的外部限制，对科研活动的规范应优先借助科技系统自身。借助科技伦理规范科技本身，此谓科技系统的自我反身性。长期以来，人们认为科研不应存在禁区，因为科学研究本身是一种求真的活动，依赖一个自由探索的科研环境。如若事先设定禁区，将会破坏科学研究的求真本性。但随着现代科学的兴起，知识的发现不再被认为是最终目的，科学的成功可能就是危害的开始。美国《科学》杂志指出，现代科学引发的科学与社会责任、科学与伦理、科学与现代性等问题，正以前所未有的速度与规模引起人们的注意。[32]科学并非全然有益，一些科学研究的危害性甚至胜过其学术性。人们逐渐认识到，科技并非文明，科研活动也应受到规范，科技伦理应运而生。人工智能活动作为科技活动的一种，当然应遵守人工智能科技伦理。

人工智能法的科技法属性也意味着，我们在规范科技活动的同时应规定适当的科技促进型制度。人工智能的核心要素是算法、算力与数据，但人工智能法并不等同于人工智能要素法。若将人工智能立法简单拆分为人工智能要素的立法，围绕各个要素设计一般性规则，不但会消解人工智能法的立法目的，也会模糊人工智能法与《个人信息保护法》《数据安全法》等法律的关系。不能因为人工智能的核心要素是算法、算力与数据，就围绕各个要素面面俱到地制定规则。所应思考的毋宁是，阻碍人工智能发展的障碍为何、我国未来的《人工智能法》又应如何适当地设计规则以充分发挥制度的破壁效果。目前较为清晰的是，数据资源的汇集与适用

是影响人工智能发展的关键性问题。[33]中国社会科学院发布的《人工智能示范法（专家建议稿）》第 18 条、中国政法大学等高校合作起草的《中华人民共和国人工智能法（学者建议稿）》第 20 条，均规定了数据要素供给制度，强调国家应支持建设人工智能领域基础数据库和专题数据库，促进数据资源高效汇聚和共享利用，鼓励引导相关主体开展大数据与人工智能技术协同研发等。[34]我国未来的人工智能立法，应规定数据使用规则，适度突破既有的个人信息保护规则、著作权保护规则，满足人工智能训练的数据需求。

2.作为应用法的人工智能法

人工智能复杂、多样的场景化应用增加了统一立法的难度。人工智能赋能不同应用场景，引发的法律关系并不相同。以人脸识别为例，如果人脸识别技术被用于门禁、电子护照、自动支付，涉及的法益包括出行自由与财产安全等；但若人脸识别技术被用于一般性的监控，则主要涉及自由与安全之间的矛盾。[35]自动决策算法在公私不同领域中的应用，引发的法律问题也不一样。商业领域的自动决策算法应用容易引发算法黑箱与歧视问题。例如，招聘人工智能可能有意识地排斥特定地域的应聘者，将地域歧视程序化。[36]公权力运用决策型算法的，则会直接对个人的基本权利造成影响。例如，以“秒批”为代表的自动行政算法极大地提升了行政效率，但也在一定程度上侵犯了公民的人身自由和知情权。可见，人工智能在公私领域应用涉及的价值各异，统一的规范设计并不容易。

在很长的一段时间内，思想家偏好一种本质论的思维方式，即通过界定“事物本质”来寻找其发展规律，运用规律规范事物本身。遗憾的是，试图抓住本质、化繁为简的努力往往不易成功，很多时候是表面上似乎对认识对象一目了然了，但是实际上却并没有真实反映复杂社会的实际情况，反倒使得认识对象被过度简化。所以，现代认识范式越来越偏爱非本质论，即通过揭示事物的复杂性、多样性，在全面了解事物不同面相的基础上解释与调整事物。[37]以经济学为例，复杂经济学理论指出，古典均衡理论过于理想化和理性化，扭曲了现实世界。现代经济学批判以往经济模型的过度简化，认为经济不是确定的、静态均衡的，而是依赖于过程的、有机的、永远在进化的。[38]笔者认为，欧盟采取风险管理单一进路规范人工智能活动，认为风险是确定的与可预测的，一定程度就是在将复杂世界简单化与静态化。单一理论是无法规范复杂、多场景的人工智能应用的，如果按照单一理论设计规则，难免会产生规制过严或过松的问题。鉴于人工智能多样的应用场景，人工智能赋能应用规范不应寻求简单的、单一的规范框架，而应充分重视事物的复杂性。

我国目前存在两个版本的人工智能法建议稿。中国社会科学院发布的《人工智能示范法 2.0（专家建议稿）》规定了人工智能支持与促进制度，人工智能管理制度，人工智能研发者、提供者义务以及人工智能综合治理机制；中国政法大学等高校合作起草的《中华人民共和国人工智能法（学者建议稿）》规定了发展与促进、使用者权益保护、开发者与提供者义务规范、监督管理、特殊应用场景、国际合作等。[39]无论是哪一个版本，均未采取单一的风险管理路径或某种单一理论模型规范人工智能赋能活动。笔者认为，不同的人工智能活动所涉问题分属不同的领域，涉及的主体结构、利益关系也有所不同。人工智能赋能应用活动具有高度场景化特征，没有任何一个“正确”的预期模型可以被假定为共同知识。因此，人工智能赋能应用活动的规范，不应过度追求理论化与体系性，而应在充分了解现实问题的前提下，设计能够满足场景化应用与动态调整需求的治理结构。

四、复式立法进路下人工智能规范框架的展开

人工智能活动具有科学性与赋能性，我国未来的人工智能立法也应在科技法与应用法复式定位下展开。一部立法具有双重定位，无疑极为考验立法者的智慧。一个简单的、逻辑清晰的治理框架虽然符合形式美感，但可能削足适履，不能有效地调

整规范对象。作为科技法的《人工智能法》应重在将科技伦理内化于人工智能研发活动中，同时打破制度壁垒，促进人工智能科技的发展；作为应用法的《人工智能法》则应关注科技赋能导致的功能异化现象，借助灵活的规范配置，满足多样的规范需求。

（一）科技法定位下的人工智能研发伴生性规范

人工智能研发活动属于专精科技活动，具有科学性。与之相应，对人工智能研发活动的规范，不能忽视科技系统独有的调整方式。此外，以科技活动为规范对象的人工智能法，应充分发挥科技促进法的功能，破除人工智能发展的制度障碍，促进人工智能科技成果转化。

1.科技伦理义务化

科技不同于自然，自然中万事万物紧密关联，科技则是操作系统的因果性闭合。[40]科技系统的内在封闭性意味着，只有本系统成员才能充分理解其内部发生的意义沟通过程。计算机科学家最了解人工智能研发中的危险，也处于控制危害的最佳位置。作为科技法的人工智能法，应关注研发过程，要求科学家遵守科技伦理。

科技伦理是科技系统对科研活动的自我调整方式。科技伦理可以输送更具时效、更加贴合技术发展与商业模式的行为规范，实现尊重人工智能发展规律、促进人工智能场景创新与立法监管相协调，增强立法的社会适应性。[41]国家新一代人工智能治理专业委员会于 2021 年发布的《新一代人工智能伦理规范》就确立了强化自律意识、提升数据质量、增强安全透明和避免偏见歧视四项研发规范。唯须注意，伦理原则只有具体化、义务化，才能真正发挥作用。如果没有通过立法确定具体的人工智能活动规则，人工智能伦理原则将难以落地。[42]法秩序应通过设计研发伴生性规范的方式，将科研伦理内化于科研过程。我国未来的人工智能法应规定记录义务、报告义务、安全管理和伦理委员会等制度。囿于篇幅，下文主要介绍研发人员应承担的记录和报告义务。

记录是科技系统自我观察与调试的基础。人工智能活动引发的风险具有不可预测性，唯有借助科学记录，才能在一定程度上理解正在进行的科研活动。欧盟委员会于 2020 年发布的《人工智能白皮书——追求卓越和信任的欧洲方案 2020》就明确指出，人工智能设计者和运营者应当记录并保存下列信息：训练和测试的数据集，包括对主要特征的描述及挑选数据集的方式；在合理情况下，数据集本身；有关编程和训练方法，构建、测试和验证人工智能系统的过程和技术等，包括避免歧视的相关设计。[43]在大语言模型时代，人工智能科研工作者更应承担记录义务。只有以可理解的方式记录科研流程，才有可能“控制”大模型引发的不确定性。

记录义务并非仅存在于实验室，而应贯穿人工智能系统全生命周期。考虑到人工智能的自我学习、自我成长能力，人工智能活动的记录义务应有一定的特殊性。相较于工业时代的产品，人工智能技术在投入应用后更可能实现进化，因为来自现实场景中的数据将不断刺激人工智能的自我生长。基于仿生学设计的“种子人工智能”（Seed AI）能够不断改良自身。种子人工智能首先通过试验和试错、信息采集以及程序员协助等方式理解自己的运行逻辑，然后通过建立新算法与结构实现“递归性自我提升”（recursive self-improvement），从而获得自我进化能力。[44]从某种意义上说，整个社会都是人工智能系统的进化场所。欧盟《人工智能法》第 12 条第 1 款明确要求高风险人工智能系统应具备在运行时自动记录事件的能力，第 2 款则强调人工智能开发者将人工智能产品投入市场后需要承担产品追踪记录义务。只要人工智能系统具有自我学习能力，研发者就应承担持续的记录义务，以实现对人工智能系统的全生命周期监测。

报告义务与记录义务相辅相成，是同一硬币的两面。如果根据记录发现人工智能模型存在错误或缺陷，研发人员应及时向监管机构汇报。欧盟《人工智能法》第 62 条第 1 款要求高风险人工智能系统的提供者发现严重故障时，应立即向监管机构进行汇报，报告时间应在发现严重故障之日起 15 日

内。当强人工智能有望实现时，科研工作者更应及时报告，因为强人工智能技术可能是人类最后一个发明，会给作为发明者的人类带来巨大危险。当然，也有人指出，强人工智能的到来尚遥遥无期，人工智能末世论过于夸大人工智能的危险。[45]对此，或许只有时间才能分辨对错。真正需要思考的问题是，我们是否愿意接受因技术蝶变而自我毁灭的可能。当奇点时刻来临时，不应仅由科学家决定人类的命运，而应让包括科学家在内的全人类共同作出选择。但要让研发者之外的其他人也获得决定权，就必须使其能够实时了解研发进度。因此，人工智能研发者应负有重大事项报告义务，以使监管机关可以据此及时介入人工智能科研活动，防止系统发生整体性崩坏。

目前，互联网监管部门正在尝试通过算法备案的方式强化对人工智能活动的监管。[46]但相较而言，算法备案不如记录与报告义务那么契合专精科技活动的科学性。通过算法备案的方式规范人工智能活动，并不符合科技法规范模式。算法备案实质是一种权力机关试图深入到科技系统内部、直接监管人工智能设计与运行的有益尝试，旨在获取平台设计部署的具有潜在危害和风险的算法系统的相关信息，以固定问责点，为今后的行政监管提供信息基础。[47]但是，备案可能成为变相的审批，不当干扰科技研发。实践中，部分监管部门以备案之名行审批之实，过度侵蚀科技系统的自主性。欧盟 1995 年颁布的《个人信息保护指令》（Data Protection Directive）第 18、19 条曾规定个人信息控制者和处理者使用自动化算法的备案义务。但在制定欧盟《通用数据保护条例》（GDPR）的过程中，欧盟委员会就指出备案义务增加了企业的官僚主义负担，并主张废除一般性的备案义务，改为要求全面记录个人信息处理活动；一旦监管机构要求算法使用人提供记录，算法使用人有义务及时、全面提供相应的记录。[48]2016 年通过的欧盟《通用数据保护条例》采纳了欧盟委员会的建议，于第 30 条规定中以记录和报告义务取代《个人信息保护指令》中的备案义务。此外，人工智能大语言模型具有不断进化的能力，将静态的、一时的算法予以备案，也不足以帮助监管部门了解算法的后续进化。更优的路径是强化人工智能开发者的持续记录与报告义务，借助科学系统自身的控制阀门实现治理目标。

2.建立促进人工智能科技发展的数据制度

《人工智能法》以科技活动为调整对象，应在规范之余设计促进型制度，助力人工智能科技发展。数据利用问题是制约人工智能发展的卡脖子问题，不论大模型设计的技术水平有多高，数据训练数量与质量均对 AI 性能具有决定性影响。依数据来源主体不同，数据可以分为个人数据与非个人数据。目前人工智能训练使用个人数据的，只有在符合《个人信息保护法》规定的合法性基础的前提下才能实现，这严重限制了人工智能的数据训练；非个人数据的利用虽然无需受到个人信息保护法律的拘束，但也面临“数据孤岛”“数据垄断”等问题，加之知识产权制度的影响，人工智能训练难以汇聚利用商业数据、中国知网等知识平台的高质量数据。[49]

首先，人工智能立法可以借助可期待性同意规则，允许合理利用个人数据进行人工智能训练。《个人信息保护法》第 13 条第 1 款规定了七项处理个人信息的合法性基础，其中“个人的同意”是处理个人信息的核心规则。[50]依据第 14 条规定，同意必须由个人在充分知情的前提下自愿、明确作出，但一方面，人工智能训练需要海量的个人数据，无法事先一一获得个人的同意；另一方面，同意机制在人工智能时代也可能成为个人的负担——个人信息主体在无法充分理解人工智能活动的情况下，被迫面临信息过载和决策过频的问题，将很难作出真正有价值的决定。[51]我国未来的人工智能立法可以尝试通过规定“可期待性同意”的方式，在减轻个人负担的同时，允许人工智能系统在符合期待的情境下收集与处理个人信息。早在 2004 年，美国学者就提出“情境诚信理论”，认为个人信息保护应当根据不同的情境而有不同的期待。如果行为不合期待，即便有个人明确的同意也构成对个人信息的侵犯；反之，即便个人没有事先明确同意，个人信

息处理活动也是合法的。[52]例如，智能家居机器人在征得购买者同意处理其个人信息时，当然还会处理购买者家庭其他成员（如未成年人）、偶然使用者（如访客）等个人信息，此时人形机器人的数据处理行为应是符合期待的。借助“可期待性同意”规则，可以一定程度上柔化《个人信息保护法》中的同意规则的刚性，推动人工智能通过收集与处理个人数据实现科技蝶变。

其次，人工智能立法应借助数据访问权打破数据孤岛，并适当纾解人工智能利用非个人数据的知识产权限制。数据不会被耗尽，且能够为实现不同目的而被反复利用与共享，数据的这一属性使得数据共享作为常态成为可能。但在技术壁垒与商业模式的影响下，数据集中于大型平台之上，最终容易导致数据孤岛和数据垄断。对于个人数据，尚可以借助《个人信息保护法》第 45 条第 3 款规定的数据可携带权实现数据流转；但对于非个人数据的流转，却不存在明确的规则。监管部门要求大型平台之间“互联互通”，但有过分侵犯营业自由的嫌疑；要求强强联合，却可能进一步促成数据垄断。[53]2022 年公布的《欧盟数据法》专门规定了数据访问权（right of access to data），允许个人携转与产品或服务有关的非个人数据。[54]我国的人工智能立法可以参照规定数据访问权，将用户携转数据的对象从个人数据扩张到非个人数据，借助个人力量打破数据孤岛，促进数据聚合。此外，著作权也会对人工智能训练数据的汇聚和融合形成挑战。开放性网站是人工智能训练的重要数据来源。但是，开放性网站上的文字、图片、声音等很可能已经受到《著作权法》的保护。例如，微博、知乎上发表的文字或问答，微信、小红书、抖音上用户上传的音乐、图片、视频，在达到独创性的门槛后，都可能获得著作权保护。一旦人工智能企业利用这些内容数据，就有可能构成著作权侵权。[55]为了鼓励人工智能科技发展，日本政府官员表示，日本法律不会保护人工智能集中使用的原始材料版权。[56]但笔者认为，一概允许人工智能使用他人作品进行训练，未免过于极端了。更为妥适的做法是借鉴欧盟 2019 年《单一数字市场版权指令》第 4 条的规定，一方面规定以人工智能训练为目的使用作品构成著作权保护的例外，另一方面允许著作权人以可机读的方式明确反对人工智能系统使用其作品进行训练。考虑到人工智能将使用海量的作品进行训练，我国未来的《人工智能法》还可以借鉴欧盟《人工智能法》第 53 条第 1 款第 c 项的规定，要求相关主体制定专门性的符合著作权法的政策，帮助著作权人行使反对权。

（二）应用法定位下的人工智能赋能规制型制度

科学研究的主要目的是发现知识，控制危险仅为其考虑的次要因素，而主要目的会天然地弱化次要因素。例如，企业的主要宗旨是营利，企业文化形成仅为企业的次要追求，当主旨与次要目的发生冲突时，企业会为了营利而放弃建设或改变企业文化。同样，科技系统可能会为了促进科技进步，而忽视权益保护、社会正义等价值，因此，法律作为社会回应新型挑战的有力工具，有必要进行更为积极的干预，人工智能立法因而迫在眉睫。倘若人们将法律系统视为一种应对危机的方式，那么法律系统就是全社会的免疫系统。[57]但是免疫并不总是有益，有时会徒增烦恼。法律规范可能因过于刚性而阻碍人工智能产业的发展。是以，对人工智能应用的规范既需要借助法律系统，也应留出必要的接口推行实验主义治理，构造一种灵活的人工智能赋能规制型框架。

1.规范人工智能多场景应用的权利义务机制

合法与非法是法律系统的基本符码，只是人工智能的应用呈现为从场景到场景的现象罗列，增加了设计统一规则的难度。鉴于法律系统系借助抽象的权利义务制度调整复杂的生活，人工智能立法应侧重于识别与总结相关主体的权利与义务类型。[58]

（1）人工智能系统相对人的应有权利

为了捍卫人的中心地位，人工智能系统相对人应享有一系列保护性权利。欧盟在起草《通用数据保护条例》时就已经明确指出，采取基于风险的规制路径无法充分支撑起欧盟数据保护的法律框架，

无论在数据处理过程中产生的风险程度如何，法律都应赋予数据主体权利。[59]相较于个人信息保护，人工智能涉及的问题更为复杂、更加场景化，因而更应重视私权的作用。

首先，人工智能系统相对人的知情权应受法律保护。知情权是确立以人为本的人工智能善治的前提与基础，不论是在何种场景下，个人的知情权均应受到尊重。如果个人都不清楚是否已经进入人工智能生态系统，就很难产生捍卫个人权利的意识。人工智能相对人应有权了解自己的信息是否在被人工智能系统处理，应有权获知人工智能系统的预设功能、局限性、不良影响等信息。当人工智能系统具有一定程度上的操纵性时，系统提供者更应将这一情况告知相对人，使其意识到自己的自由意志有被扭曲的可能。即便是治疗性医疗人工智能，在修复心理创伤之前，也应告知病患，尊重病患的自主决定权（《民法典》第 1219 条）。

其次，个人在了解相关信息后，是否享有解释请求权、应用拒绝权等权利，则应视场景而定。其一，不同类型的人工智能系统对应不同的个人权利。应用场景中的人工智能活动大致可以分为决策型与辅助型两类。决策型人工智能代替人快捷地作出判断与决定，典型如信用评级（贷款或信用卡发放）、防疫健康码、“秒批”、税务抵扣系统等。辅助型人工智能仅提供辅助支持作用，如个性化推荐、医学图像处理、智能客服机器人等。决策型与辅助型人工智能系统在不同应用场景中对相对人的影响不同，权利配置也应有所不同。决策型人工智能系统直接影响相对人的法律利益，相对人应有权利请求解释决策是如何作出的；辅助型人工智能系统并不直接作出影响相对人利益的决定，但可能潜移默化地影响相对人的思维方式，因此相对人应有权利事先拒绝该系统的应用。是以，个人的解释请求权应主要针对决策型人工智能系统，应用拒绝权则主要以辅助型人工智能系统为对象。其二，无论是解释请求权还是应用拒绝权，均应区分公私应用场景分别判断权利的适用空间。以解释请求权为例，公权力借助人工智能系统进行行政或司法行为的，相对人应有权请求解释人工智能系统的具体决策；商业机构使用人工智能系统进行商业活动的，相对人是否享有解释请求权，则应综合衡量解释可能性以及商业秘密保护等因素进行判断。[60]当公权力运用人工智能系统进行决策时，如果不能解释决策，公共行为的正当性和合法性都将遭受质疑。因为与提升行政与司法效率相比，公民基本权利保护的价值位阶更高。与之不同，商业人工智能系统的逻辑、参数、特征的权重以及分类等是企业的商业秘密，未必应屈从于个人的算法解释请求权。德国联邦最高法院在 2014 年的判决中明确指出，数据主体不得请求披露权重、评分公式、统计值和参考组等信息，因为这触犯了企业的商业秘密，披露企业的商业秘密也明显不符合立法目的。[61]当个人要求解释商业自动决策算法的决定时，算法解释请求权如何与保护商业秘密的法律要求相协调，将是司法审判的难点。

最后，我国未来的《人工智能法》还应专门规定请求人工沟通的权利。只有保证个人享有表达意见、获得人为干涉的权利，人才不会沦为机器的客体。欧盟《通用数据保护条例》第 22 条第 3 款专门规定了算法相对人请求人工干预的权利。相较而言，我国《个人信息保护法》第 24 条第 3 款仅规定请求说明算法和拒绝算法决定的权利，并未规定人工沟通的权利。在人工智能时代，受影响个人有权与机器背后的人进行有意义的沟通，是捍卫人的主体地位的基本要求。我国未来的人工智能立法应专门规定人工智能系统相对人享有人工沟通权。

（2）人工智能系统提供者与使用者的不同义务

人工智能系统相关义务主体大致可分为提供者与使用者两类，由于二者对作为赋能工具的人工智能系统的影响不同，所应承担的义务也应有所不同。人工智能系统提供者负责设计开发产品并将之投入市场，应承担信息公开、人工监督等义务；人工智能系统使用者则因可以影响具体的输出结果，应承担谨慎使用、保存日志等义务。

第一，不论是决策型还是辅助型人工智能系统，也不论应用于何种场景，人工智能系统提供者均应一般性地承担特定的法律义务。这些义务包括但不限于信息公开、人工监督、保障系统稳定性等。首先，人工智能系统提供者应承担信息公开义务，以使下游合作者和用户能够及时了解系统相关信息。这些信息主要包括提供者的身份和联系方式、人工智能系统的功能及其局限性、测试结果、对目标人群可能的不利影响以及如何进行系统维护等。人工智能系统提供者应通过说明性文件（技术文件）的方式，将上述信息告知相对人。其次，人工智能系统设计应留有适当的人机交互界面，以便对人工智能系统进行有效的监督。人工监督机制旨在及时发现人工智能系统的功能异常和性能突变迹象，纠正自动化偏差，手动控制或逆转输出结果。当出现重大隐患时，人工智能系统提供者应有义务“一键关闭”人工智能系统，避免发生不可逆的后果。再次，人工智能系统提供者应当维护人工智能系统的稳定性和安全性，尤其是确保人工智能系统具有自我复原能力。恶意第三方可能通过“脏数据”、系统漏洞等试图改变人工智能系统的运作模式、性能以及输出结果。人工智能系统提供者可以有针对性地通过提供备份、补丁和安全解决方案等技术方案保护网络安全。最后，我国作为《联合国残疾人权利公约》（UNCRPD）的签署国，有义务确保残疾人同等地使用人工智能系统。在人工智能时代，弱势群体同样有权不受限制地使用人工智能技术。人工智能服务提供者应当在系统设计时就考虑到弱势群体的需求，提供必要措施，以使弱势群体不至于被技术排除在外。

第二，人工智能系统使用者应承担谨慎使用、保存日志等义务。人工智能系统的提供者与使用者并非同一主体的，人工智能系统使用者直接操作人工智能系统，系处于影响系统结果和监测程序运行的最佳位置，因而应承担与之相称的法律义务。其一，人工智能系统使用者应谨慎使用人工智能系统。使用者输入数据可能影响到系统功能的，应确保输入数据的正当性。例如，生成式人工智能以“用户输入+机器输出”的模式提供服务，生成内容的性质、价值取向很大程度上取决于用户输入指令。人工智能系统使用者应当遵守人工智能系统的预设功能，不能通过模糊词等欺骗性手段实现非法目的。[62]其二，如果日志对诊断系统的运行状态和故障是不可或缺的，人工智能系统使用者就有保存相关日志的义务。只是考虑到存储成本问题，日志保存宜设置期限限制（如六个月）。其三，人工智能系统使用者如果发现人工智能在具体场景中可能产生歧视、侵犯人格尊严等问题，应当暂停使用该系统，并将问题反馈给人工智能系统提供者。如果存在重大隐患，应当同时上报国家监管机构，以防止发生不可逆的后果。

我国未来的人工智能立法除了规定上述一般性的义务外，还可以挑选重要的具有成熟监管经验的人工智能场景，有针对性地规定人工智能系统提供者和使用者的特殊义务。例如，我国未来的人工智能立法可以考虑对公权力使用人脸识别等人工智能系统作出专门规定。反之，如果一些场景中的人工智能相关主体义务尚有争议，不妨适当留白，交由监管机构出台专门性法律文件进行规范。[63]

2.调整人工智能复杂应用活动的实验主义治理

新兴科技对治理产生的挑战主要体现为未知与不确定性。未知是指决策者可能并不了解真实的、不断变化的问题；不确定性则是指决策者不具有解决问题的能力，需要不断研究和改进治理方案。[64]即便在充分调研的基础上配置权利义务制度，人工智能复杂的、多场景的应用活动也可能使得一时有效的规则转瞬变成科技发展的障碍。是以，法律常常面临与新兴技术的步调失调问题。为了破解这一难题，我国未来的《人工智能法》可以考虑推行实验主义治理模式，构造试错与纠错的动态机制。

实验主义治理（Experimentalist Governance）起源于对欧盟治理政策的总结性思考和提炼。[65]实验主义治理大致包括四项内容：大致的框架目标、参与者的自由裁量、基于同行评议的动态评估，以及根据评估结果的反馈修正。具体而言，决策机构在充分听取利益攸关者的意见后，确立一个开放式框

架性目标；授权相关机构以较大的自由裁量权，根据具体情况调整策略；负责机构应定期汇报治理绩效，并经由同行评估判断妥适性；负责机构如果没有取得良好进展，则应当根据评估结果提出合理的改进计划。在该治理模式下，目标是可变的，既定的规则是不存在的，它们都会基于评估结果被修正，通过在临时性目标设置与修正之间反馈迭代、循环往复，经由“共同学习”最终寻找妥适的应对挑战方案。[66]实验主义治理强调构建多元性、开放性和互动性的治理系统，能够弥补传统科层式治理模式的主体单一性、体系封闭性和过程单向性等不足，并更好地应对不断发展、调整的人工智能应用活动带来的挑战。

实验主义治理突出体现为一定程度的纵向放权，使得监管机构能够进行监管实验、积累监管经验。在实验主义治理模式下，立法者设计人工智能监管的大致目标，授予监管机构自由裁量权，监管机构定期评估并汇报治理绩效，并根据相关主体的建议调整监管策略。监管沙箱（Sandbox）是推进实验主义治理的典型设计。监管沙箱是一种由监管机构依据法律规定设立的受控测试环境，在限定时间内允许人工智能系统进行开发与测试。人工智能活动即便违反现行法律法规，只要符合监管沙箱的要求，相关人员也不会被问责。英国科学创新与技术部指出，监管沙箱能够帮助迅速将新产品和服务推向市场，产生经济和社会效益；检验监管框架在实践中的运行情况，揭示需要解决的创新障碍；并确定监管框架需要适应的技术和市场的调整方向。[67]公权力机关基于一些特殊的考虑，会希望在特定地域或领域加速人工智能产业的发展。例如，日本就专门划出特定地域和场景布局人工智能产业，如福冈（道路交通）、关西（无线电）、京都（数据保护）、筑波（安全治理和税收规制）等。我国未来的人工智能立法应授权监管部门在特定地域与领域设立监管沙箱，从而摆脱“操之过急”或“听之任之”的弊端。监管部门可以根据评估结果，适当调整监管沙箱政策，在摸索中寻找妥适的治理手段。此外，立法还可以通过授权监管机关出台专门规范性文件的方式推行实验主义治理。在高新科技领域，中小企业往往是创新的主力。正如凯文·凯利指出的，未来在人工智能领域大放异彩的企业，大概率不会是现在的大型企业，而是某个不起眼的小公司。[68]欲使中小企业完成蝶变，就应在制度层面提供额外的支持。如同《个人信息保护法》第 62 条第 2 项授权国家网信部门出台专门针对小型个人信息处理者的规则与标准一样，我国未来的人工智能法也可以赋权监管机构出台专门的规范人工智能中小企业的文件，以促进科技创新。例如，监管机构可以授予中小型人工智能企业对人工智能监管沙箱的优先访问权；可以提供专项资金，解决中小企业的融资难题；可以适当地降低义务标准，或者在充分保障个人权益的基础上，提供一定程度上的责任豁免等。监管机构应定期评估规范性文件的效果，并根据同行评估不断调整方案，以真正满足中小型科技企业的诉求。除上述规则外，日落规则、智能预期草案等设计，都可以成为贯彻实验主义治理的有益尝试。[69]

五、余论

目前世界正处于第四次工业革命全面来临前夕。第一次工业革命和第二次工业革命都是围绕动力提升展开，第三次工业革命是信息革命，第四次工业革命是智能革命，与第三次工业革命既有关联，也有本质不同。第四次工业革命是对人类智能的模拟与提升，围绕智能展开，其核心是人工智能技术的研发与赋能推广。中国未来的人工智能立法必然应以促进人工智能可控发展为目标，否则中国将再次落后于世界浪潮。

欧盟《人工智能法》采取风险管理路径，形成了以监管为核心的规范框架。但欧盟采取风险管理单一进路规范人工智能活动，认为风险是静态的、确定的与可预测的，并不符合复杂、动态发展的世界。更为科学的做法应是基于人工智能活动的双重属性，明确人工智能法的科技法与应用法复式定位，在规范人工智能活动的同时最大限度地促进人工智能技术与产业的发展。笔者相信，尊重科技自主、

强调灵活规范的中国《人工智能法》将成为人工智能立法的一种新范式，为世界人工智能治理提供来自东方大国的智慧。

参考文献

[1] See Margot E. Kaminski, Regulating the Risks of AI, Boston University Law Review, Vol.103:1347, p.1347-1411 (2023).

[2] 参见刘权：《数字经济视域下包容审慎监管的法治逻辑》，载《法学研究》2022 年第 4 期，第 37-51 页。

[3] 例如，在数字化时代，无法适应智能手机的老人遭遇“数字鸿沟”，有被排挤出社会的危险。工业与信息化产业部印发了《互联网应用适老化及无障碍改造专项行动方案》（工信部信管〔2020〕200 号），在全国范围内组织开展为期一年的互联网应用适老化及无障碍改造专项行动。该项举措一定程度上改善了老年人的数字生存困境，但并未从根本上解决问题。

[4] See William Boyd, Genealogies of Risk: Searching for Safety, 1930s-1970s, Ecology Law Quarterly, Vol.39:895, p.912 (2012).

[5] See Douglas A. Kysar, The Public Life of Private Law: Tort Law as a Risk Regulation Mechanism, European Journal of Risk Regulation, Vol.9:48, p.52 (2018).

[6] See European Parliament, The Precautionary Principle: Definitions, Application and Governance, at https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/573876/EPRS_IDA(2015)573876_EN.pdf (Last visited on Aug. 3, 2024).

[7] 参见黄宁燕：《“ChatGPT 之父”提出未来人工智能监管框架》，载《科技中国》2023 年第 8 期，第 98 页。

[8] See Cameron A. MacKenzie & Christopher W. Zobel, Allocating Resources to Enhance Resilience, with Application to Superstorm Sandy and an Electric Utility, Risk Analysis, Vol.36: 847, p.859 (2015).

[9] See Ortwin Renn & Andreas Klinke, Risk Governance: Concept and Application to Technological Risk, in Adam Burgess, Alberto Alemanno & Jens Zinn eds., Routledge Handbook of Risk Studies, Routledge Press, 2016, p.204-215.

[10] See Bridget M. Hutter, A Risk Regulation Perspective on Regulatory Excellence, in Cary Coglianese ed., Achieving Regulatory Excellence, Brookings Institution Press, 2016, p.101-114.

[11] See David W. Hobson et al., Applied Nanotoxicology, International Journal of Toxicology, Vol.35:5, p.6 (2016).

[12] See Morten Broberg, Risk Regulation and the Future: On the Need for Helping Vulnerable Societies to Adapt to the Consequences of Climate Change, European Journal of Risk Regulation, Vol.8:101, p.101-105 (2017).

[13] 参见张凌寒：《生成式人工智能的法律定位与分层治理》，载《现代法学》2023 年第 4 期，第 126-141 页。

[14] See W. Kip Viscusi & Richard J. Zeckhauser, Regulating Ambiguous Risks: The Less than Rational Regulation of Pharmaceuticals, Journal of Legal Studies, Vol.44:387, p.387-422 (2015).

[15] See Wendy E. Wagner, The Science Charade in Toxic Risk Regulation, Columbia Law Review, Vol.95:1613, p.1627-1628, 1678 (1995).

[16] 参见[德]乌尔里希·贝克：《风险社会：新的现代性之路》，张文杰、何博闻译，译林出版社 2022 年版，第 46 页。

[17] See The National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), at https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf (Last visited on Oct. 17, 2023).

[18] Vgl. Markus Thiel, „Deepfakes“ – Sehen heißt glauben?, ZRP202 (2021), S. 203.

[19] See Department for Science, Innovation & Technology, A Pro-Innovation Approach to AI Regulation, 2023, p.12.

[20] See Natali Helberger & Nicholas Diakopoulos, ChatGPT and the AI Act, Internet Policy Review, Vol.12:1, p.1-6 (2023).

[21] See John Durant, Once the Men in White Coats Held the Promise of a Better Future, in Jane Franklin ed., The Politics of Risk Society, Polity Press, 1998, p.73.

[22] See Daniel A. Farber, Uncertainty, Georgetown Law Journal, Vol.99:901, p.909 (2011).

[23] 参见［英］彼得·本特利：《计算机：一部历史》，顾文天译，电子工业出版社 2015 年版，第 255-284 页。

[24] See Gary Drenik, Large Language Models Will Define Artificial Intelligence, at https://www.forbes.com/sites/garydrenik/2023/01/11/large-language-models-will-define-artificial-intelligence/?sh=33b50d6ab60f (Last visited on July. 27, 2023).

[25] 参见［美］亨利·基辛格、［美］埃里克·施密特、［美］丹尼尔·胡滕洛赫尔：《人工智能时代与人类未来》，胡利平、风君译，中信出版社 2023 年版，第 15 页。

[26] See Chris Olah et al., The Building Blocks of Interpretability, at https://distill.pub/2018/building-blocks/ (Last visited on Jan. 1, 2024).

[27] 参见龙卫球：《科技法迭代视角下的人工智能立法》，载《法商研究》2020 年第 1 期，第 57-72 页。

[28] See Amanda J. Sharkey & Noel Sharkey, Granny and The Robots: Ethical Issues in Robot Care for The Elderly, Ethics and Information Technology, Vol.14:27, p.27 (2012).

[29] See European Parliament, The Ethics of Artificial Intelligence: Issues and Initiatives, PE634.452, March 2020, p.18.

[30] 参见林洹民：《人形机器人的操纵性风险及规范进路》，载《东方法学》2024 年第 3 期，第 159-170 页。

[31] Vgl. Niklas Luhmann, Rechtssoziologie, 4. Aufl. 2008, S. 236.

[32] See Rosemary Chalk ed., Science, Technology, and Society: Emerging Relationships, American Association for the Advancement of Science, 1988, p.11.

[33] 我国台湾地区于 2024 年发布的“人工智能基本法（草案）”第 15 条就专门强调，应建立资料开放、共享与再利用机制，提升人工智能使用资料之可利用性，提升人工智能使用资料之质量与数量。

[34] 参见《〈人工智能示范法 2.0（专家建议稿）〉发布》，载微信公众号“网络与信息法学会”，2024 年 4 月 16 日上传；《〈人工智能法（学者建议稿）〉全文发布》，载微信公众号“人工智能产业发展联盟 AIIA”，2024 年 3 月 20 日上传。

[35] 关于公权力在公共场所使用实时人脸识别系统的讨论，参见赵精武：《人脸识别技术应用的利益权衡与合法性认定》，载《法律科学》2024 年第 1 期，第 100-110 页。

[36] 参见时婷婷：《女孩因“河南人”应聘被拒案开庭 浙江喜来登被判道歉赔偿 1 万元》，载澎湃新闻网，https://www.thepaper.cn/newsDetail_forward_5064609，2024 年 1 月 31 日访问。

[37] 参见龙卫球：《人工智能立法规范对象与规范策略》，载《政法论丛》2020 年第 3 期，第 95-106 页。

[38] 参见［美］布莱恩·阿瑟：《复杂经济学：经济思想的新框架》，贾拥民译，浙江科学技术出版社 2018 年版，第 4 页。

[39] 参见前注 [34]，《〈人工智能示范法 2.0（专家建议稿）〉发布》；前注[34]，《〈人工智能法（学者建议稿）〉全文发布》。

[40] 参见［德］尼克拉斯·卢曼：《风险社会学》，孙一洲译，广西人民出版社 2020 年版，第 129-133 页。

[41] 参见陈亮：《人工智能立法体系化的困境与出路》，载《数字法治》2023 年第 6 期，第 11 页。

[42] See Brent Mittelstadt, Principles Alone Cannot Guarantee Ethical AI, Nature Machine Intelligence, Vol.1:501, p.503 (2019).

[43] See European Commission, White Paper on Artificial Intelligence - A European Approach to Excellence and Trust, Brussels, Feb.19, 2020, COM (2020) 65 final.

[44] 参见［英］尼克·波斯特洛姆：《超级智能：路线图、危险性与应对策略》，张体伟、张玉青译，中信出版社 2015 年版，第 36-37 页。

[45] See Kate Crawford & Ryan Calo, There is a Blind Spot in AI Research, Nature, Vol.538:311, p.312 (2016).

[46] 例如，《互联网信息服务算法推荐管理规定》第 24 条第 1 款规定，具有舆论属性或者社会动员能力的算法推荐服务提供者应当履行备案手续。

[47] 参见张凌寒：《网络平台监管的算法问责制构建》，载《东方法学》2021 年第 3 期，第 22-40 页。

[48] Vgl. Spiros Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), Datenschutzrecht, Nomos Verlag, 1. Aufl. 2019, S. 804.

[49] 参见杨建军等：《人工智能法：必要性与可行性》，载《北京航空航天大学学报（社会科学版）》2024 年第 3 期，第 169 页。

[50] 参见杨合庆主编：《中华人民共和国个人信息保护法释义》，法律出版社 2022 年版，第 45 页。

[51] 参见林洹民：《论个人信息主体同意的私法性质与规范适用——兼论〈民法典〉上同意的非统一性》，载《比较法研究》2023 年第 3 期，第 144 页。

[52] See Helen Nissenbaum, Privacy as Contextual Integrity, Washington Law Review, Vol.79:119, p.127 (2004).

[53] 参见周汉华：《互操作的意义及法律构造》，载《中外法学》第 3 期，第 606 页。

[54] 参见丁晓东：《论数据来源者权利》，载《比较法研究》2023 年第 3 期，第 15-17 页。

[55] 参见丁晓东：《论人工智能促进型的数据制度》，载《中国法律评论》2023 年第 6 期，第 179 页。

[56] 参见《严苛版权保护阻碍 AI 技术发展？日本政府重申：AI 所用数据不受版权保护》，载新浪科技，https://finance.sina.com.cn/tech/roll/2023-06-02/doc-imyvxapa8336048.shtml，2024 年 6 月 26 日访问。

[57] Vgl. Niklas Luhmann, Das Recht der Gesellschaft, 1. Aufl. 1993, S. 565.

[58] 除了权利义务之外，人工智能致损的民事责任承担问题当然也是人工智能立法的重要问题，受篇幅所限，本文暂不讨论责任承担问题。目前学界对于人工智能致损的民事责任的讨论，参见吴汉东：《人工智能时代的制度安排与法律规制》，载《法律科学》2017 年第 5 期；冯珏：《自动驾驶汽车致损的民事侵权责任》，载《中国法学》2018 年第 6 期；郑志峰：《诊疗人工智能的医疗损害责任》，载《中国法学》2023 年第 1 期。

[59] See Article 29 Data Protection Working Party, Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks (Adopted on 30 May 2014), 14/EN WP218, p.2.

[60] 参见林洹民：《〈个人信息保护法〉中的算法解释权：兼顾公私场景的区分规范策略》，载《法治研究》2022 年第 5 期，第 48-58 页。

[61] Vgl. BGH, Urteil vom 28. Januar 2014 - VI ZR 156/13, BGHZ 200, 38.

[62] 例如，虽然 OpenAI 在使用政策中明确禁止生成恶意软件，很多使用者依然可以通过输入提示欺骗 ChatGPT 为恶意软件应用程序编写代码。

[63] 以无人驾驶汽车被动接管规则为例。2016 年 3 月修订的《维也纳道路交通公约》第 8 条增加 1 款，明确车辆系统需要能够被驾驶员接管或者关闭。2017 年 6 月，德国通过《道路交通法第八修正案》，新增的第 1a 条第 2 款也规定自动驾驶汽车应能随时被驾驶人接管。但也有研究指出，被动接管规则有悖于自动驾驶汽车作为替代型人工智能的设计初衷，只会徒增事故，且阻碍自动驾驶汽车的商业化进程。参见郑志峰：《论自动驾驶汽车被动接管规则》，载《华东政法大学学报》2023 年第 3 期，第 59-71 页。

[64] See Charles F. Sabel & Jonathan Zeitlin, Experimentalism in the EU: Common Ground and Persistent Differences, Regulation & Governance, Vol.6:410, p.410-426 (2012).

[65] See Charles F. Sabel & Jonathan Zeitlin eds. Experimentalist Governance in the European Union: Towards a New Architecture, Oxford University Press, 2010, p.1.

[66] See Jonathan Zeitlin, EU Experimentalist Governance in Times of Crisis, West European Politics, Vol.39:1073, p.1073-1094 (2016).

[67] See Department for Science, Innovation & Technology, supra note 19, 60.

[68] 参见［美］凯文·凯利：《5000 天后的世界》，潘小多译，中信出版社 2023 年版，第 21 页。

[69] 日落规则（Sunset Rules）是指特定法律只在一定时间段内有效，由此立法者可以针对特殊的问题而为“权益之计”；智能预期草案（Intelligent Anticipatory Drafting）是指立法者可以允许进行特定科技开发和应用，但是政府一旦发现其中存在问题，就可以要求企业或研究机构在一段时间内停止开发或应用。参见龙卫球、林洹民：《我国智能制造的法律挑战与基本对策研究》，载《法学评论》2016 年第 6 期，第 2 页。

(技术编辑：张清)