CAICT 中国信通院

集智 专题报告

互联网法治研究报告

(2025 年)

中国信息通信研究院互联网法律研究中心

2025年12月

版权声明

前　言

“十四五”时期，党中央对法治建设进行系统性谋划、整体性推进，互联网法治建设取得了突破性进展和历史性成就，搭建起互联网法治的“四梁八柱”，为推动互联网由大渐强，全面赋能经济社会发展提供了有力的制度保障。

2025 年是“十四五”的收官之年，我国互联网法治领域加紧落实“十四五”规划任务，在立法、执法、司法层面持续加力。针对人工智能引发的新挑战，通过加速立法迭代、强化执法协同、创新司法适用，从数据要素、人工智能应用规范、信息内容治理多维度切入，构建起适配人工智能时代的法治体系，实现创新发展与风险防控的动态平衡。

从国际来看，全球互联网领域立法围绕人工智能技术发展与风险防控展开系统性布局。人工智能综合立法持续深化，欧盟《人工智能法》等标杆性立法进入实质实施阶段，形成“综合立法+实施细则”的制度构建模式。各国在网络安全、数据治理和平台治理等方面在加强传统重点领域立法的同时，强化了应对人工智能风险挑战的制度供给。

展望未来，互联网法治可着眼加快建设网络强国、深入推进数字中国建设，抓住人工智能等技术创新、数据要素价值释放等网络领域发展的关键性、决定性因素，把握好立法的节奏和进度，为网络强国和数字中国建设的稳步推进保驾护航。

中国信息通信研究院互联网法律研究中心总结历年《互联网法

律白皮书》的研究成果和经验，系统回顾了“十四五”期间我国互联网法治领域的实践成效，梳理了过去一年国内外互联网法治发展的总体情况，深入分析我国互联网法治的最新成果和主要特点，对未来互联网法治的发展进行了展望，形成《互联网法治研究报告（2025 年）》。希望能为社会各界了解互联网领域立法最新趋势和动态提供有价值的参考。

目 录

表 目 录

一、筑基固本——“十四五”时期互联网法治建设取得显著成效

2025 年，是“十四五”规划的收官之年，面对错综复杂的国际形势和新一轮科技革命和产业变革，我国持续深化网络领域各项改革，网络大国加快向网络强国迈进。关键核心技术攻关加快推进，涌现出一批标志性科技创新产品。国产大模型在全球范围内实现了技术突破与生态影响力的双重跃升，卫星互联网发展势头迅猛，基础设施持续演进升级，建成全球最大规模信息通信网络，智能算力规模位居全球第二。截至 2025 年 6 月，我国网民规模达 11.23 亿人，互联网普及率达 79.7%。[1]互联网赋能行业数字化深入推进，服务更加普惠通达，电子商务、远程办公、远程医疗、在线教育等应用全面普及。在“人工智能+”行动推动下，新基础设施、新技术体系、新产业生态、新就业岗位等不断涌现，更好服务中国式现代化建设。量子科技、具身智能、6G 等未来产业不断培育壮大。实践证明，中国特色依法治网道路扎根中国国情、融汇国际经验，展现出强大的制度生命力。法治作为网络空间治理的基石，始终与互联网发展同步演进、同频共振。“十四五”期间，我国聚焦重点领域和技术发展前沿领域，加快制定修订相关法律法规，推动构建系统完备的网络法律体系，持续筑牢网络空间法治根基，推动立法体系在整体性、协同性与时效性方面实现全面提质升级。

体系化构建基础性法律法规。“十四五”期间，我国网络领域制定、

[1] 中国互联网络信息中心（CNNIC）：第 56 次《中国互联网络发展状况统计报告》，2025 年 7 月。

修订出台了多部法律和行政法规，网络基础立法框架不断健全，基本形成了以宪法为根本，以法律、行政法规、部门规章和地方性法规、地方政府规章为依托，以传统立法为基础，以网络内容建设与管理、网络安全和信息化等网络专门立法为主干的网络法律体系，搭建起我国互联网法治的“四梁八柱”，为网络强国建设提供了坚实的制度保障。**在专门立法方面，**制定出台《个人信息保护法》，保障个人信息安全；出台《数据安全法》，规范数据活动，完善数据安全治理体系；出台《反电信网络诈骗法》，加强立法的针对性，坚决打击遏制电信网络诈骗活动。出台《全国人民代表大会常务委员会关于修改〈中华人民共和国网络安全法〉的决定》，适应新形势新要求，充实网络安全工作指导原则，做好与相关法律的衔接，进一步完善网络安全法律责任制度，扩大域外适用情形，为维护国家网络安全、建设网络强国提供更加坚实的法治保障。公布了《关键信息基础设施安全保护条例》，落实《网络安全法》有关要求，为我国深入开展关键信息基础设施安全保护工作提供有力法治保障。公布了第一部专门性的未成年人网络保护综合立法《未成年人网络保护条例》。修订《互联网上网服务营业场所管理条例》，优化审批流程与时限，强化事中事后监督检查，优化营商环境。公布了《网络数据安全管理条例》，进一步做好相关上位法的实施，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。**在传统立法方面，**出台《军人地位和权益保障法》《无障碍环境建设法》，修订《妇女权益保障法》，加强对特殊群体数字

权利保护。修订《反垄断法》《反不正当竞争法》，根据平台经济领域竞争方式和特点，进一步明确了反垄断、反不正当竞争相关制度在平台经济领域中的适用规则。修订《反有组织犯罪法》《反间谍法》，加强在网络信息领域预防和治理犯罪，修订《保守国家秘密法》，健全涉网保密管理制度。制定《反食品浪费法》《爱国主义教育法》《慈善法》，明确在相关领域网络违法行为的边界，规范网络信息传播活动。

据全国人大常委会的统计，从 2021 年至今近五年来，我国新制定法律 36 件，修改法律 63 件次[2]，其中，包括《数据安全法》《个人信息保护法》《反电信网络诈骗法》《全国人民代表大会常务委员会关于修改〈中华人民共和国网络安全法〉的决定》四部网络领域专门立法，《民营经济促进法》《法治宣传教育法》《未成年人保护法》等含有涉网条款的立法。网络领域的专门立法和涉网立法占比约超三成。

健全重点领域和新兴领域规则实现精准治理。聚焦数字经济治理需求，我国推动网络领域配套法律规则不断迭代，实现治理能力现代化升级。聚焦新技术新业态、数据要素流通、网络市场运行、信息业务管理、网络空间生态治理等重点领域、新兴领域动态完善制度规则，形成多层次、立体化的配套规则体系，在平衡安全与发展的同时，持续释放制度效能。出台《互联网信息服务算法推荐管理规定》《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》

[2] 数据来源于国务院新闻办公室于 2025 年 9 月 12 日上午举行的“高质量完成‘十四五’规划”系列主题新闻发布会，介绍“十四五”时期坚定不移走中国特色社会主义法治道路有关情况。

《网络预约出租汽车经营服务管理暂行办法》等部门规章，完善数字经济新业态新模式相关服务的治理规则。修订《网络安全审查办法》，落实上位法的相关规定，保障网络安全和数据安全。公布了《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》《关于实施个人信息保护认证的公告》，基本构建了数据出境安全管理制度，充分释放数据要素价值，扩大高水平对外开放，为数字经济高质量发展提供法律保障。修订《电信设备进网管理办法》《非经营性互联网信息服务备案管理办法》等信息业务管理规定，进一步优化营商环境。为贯彻落实新修改的《反垄断法》，加强和改进反垄断监管执法，发布《制止滥用行政权力排除、限制竞争行为规定》《禁止垄断协议规定》《禁止滥用市场支配地位行为规定》《经营者集中审查规定》四部配套规章，不断充实网络市场公平竞争管理制度体系。公布《互联网用户账号信息管理规定》《网络暴力信息治理规定》《最高人民法院、最高人民检察院、公安部关于依法惩治网络暴力违法犯罪的指导意见》等部门规章和司法文件，健全网络综合治理体系，推动形成良好网络生态。

积极推进涉外法治输出中国制度方案。通过完善立法体系、倡导国际规则、深化跨境协作，初步构建起与网络强国地位相匹配的涉外法治框架，为全球网络空间治理贡献中国智慧。我国相继出台多部关键性立法，逐步构建网络空间涉外法治的规则体系。**一是**在相关专门立法中纳入涉外条款。这一时期出台的法律法规结合网络跨国界的特点，在相关立法中从管辖范围、具体制度、跨境执法合作等方面构建

涉外法律制度。例如《个人信息保护法》《数据安全法》《网络数据安全管理条例》等法律法规中关于适用范围的规定。又如《反电信网络诈骗法》中关于加强国际执法司法合作的规定等。**二是**积极完善数据治理领域的涉外制度规则。在《网络安全法》《数据安全法》《个人信息保护法》搭建的数据治理框架下，积极制定配套法规规章，细化安全评估、标准合同、认证等数据跨境流动规则，增强制度的可操作性。**三是**适应高水平对外开放工作需要，修订《外商投资电信企业管理规定》，降低外资进入门槛，简化流程，激发市场活力，助力构建更高水平开放型经济新体制。**四是**推进网络领域国际规则构建。发布《全球安全倡议概念文件》《全球人工智能治理倡议》《全球数据跨境流动合作倡议》等，围绕网络安全合作、人工智能发展和治理、跨境数据流动等方面，提出建设性解决思路，阐述中国方案。

严格执法保障网络空间规范有序。我国坚持严格规范公正文明执法，建立健全网络行政执法机制，稳步推进重点领域执法，保障网络空间规范有序。**一是**健全网络执法模式。我国建立完善跨部门的网络执法工作协调机制，加强线索移送、信息共享、案情通报等方面的协作配合，提升依法治网的协作能力。**二是**全面规范网络执法程序。例如，国家互联网信息办公室修订公布了《网信部门行政执法程序规定》，规范立案、调查取证、审核、决定、送达、执行等执法程序要求。工业和信息化部公布《工业和信息化行政处罚程序规定》，完善管辖制度，调整、细化普通程序等。**三是**加强重点领域执法。相关部门持续开展个人信息保护、网络信息内容生态治理、反电信网络诈骗等重点

领域的执法。在个人信息保护方面，国家互联网信息办公室会同工业和信息化部、公安部、国家市场监督管理总局开展移动互联网应用程序违法违规收集个人信息专项治理，有效整治违法违规行为。工业和信息化部持续多年组织开展移动互联网应用程序侵害用户权益专项整治，通报、下架违法违规应用程序。在网络信息内容生态治理方面，相关部门聚焦虚假信息、网络暴力、算法滥用等突出问题，持续开展“清朗”系列专项行动。在反电信网络诈骗方面，公安机关部署开展“断流”“拔钉”“斩链”等专项行动，深化对外执法合作，持续推进联合打击行动，全力挤压涉诈违法犯罪活动空间，有效遏制电信网络诈骗犯罪高发态势。

2025 年，我国互联网法治加紧落实“十四五”规划目标任务，在立法、执法、司法等方面进一步发力，针对人工智能催生的诸多网络法治新挑战，加速立法迭代，强化执法协同，创新司法适用，从数据要素价值释放、人工智能应用规范、信息内容治理等多维度，构建起适应人工智能时代的法治体系，实现创新发展与风险防控的动态平衡。

二、2025 年中国互联网法治建设情况

2025 年，我国互联网法治坚持改革和法治相统一的科学方法，以依法治网实践需求为导向，构建适配新发展环境、回应新使命新任务的现代化互联网法治体系。数据要素领域，健全相关法律制度，提升政务数据共享与开发利用法治化水平，释放数据价值。新兴领域聚焦人工智能、终端设备直连卫星等，深化治理实践，以良法善治护航行业规范发展。网络生态治理领域，不断提升治理精细化程度，优化

营商环境，规制“内卷式”竞争，增强治理效能。网络安全领域推进网络安全法修订，构建与技术产业适配、与现有法律协调的治理新格局。涉外领域健全涉外立法，深化国际交流合作，推动涉外互联网法治建设向纵深推进。

（一）数据要素治理制度持续完善，政务数据共享规则系统构建

1.出台《政务数据共享条例》

政务数据共享工作迈入法治化、规范化的新阶段。政务数据是国家重要的基础性战略资源，是公共数据资源的重要组成部分。政务数据共享作为加强数字政府建设、提升数字治理能力的关键举措，是打破“数据孤岛”的关键抓手，是加快公共数据资源开发利用的重要引擎。当前，我国政务数据共享工作仍面临着统筹管理机制需健全、供需对接不充分、支撑应用水平不足等堵点卡点。5 月，国务院公布《政务数据共享条例》，旨在推进政务数据安全有序高效共享利用，提升政府数字化治理能力和政务服务效能，全面建设数字政府。《条例》主要包括以下内容。**一是**明确总体要求。规定政务数据共享工作坚持中国共产党的领导，遵循统筹协调、标准统一、依法共享、合理使用、安全可控的原则。细化各级人民政府、政务数据共享主管部门、政府部门及其政务数据共享工作机构的职责。**二是**优化目录管理。规定政务数据实行统一目录管理，明确政务数据目录编制、发布以及动态更新等要求。确定政务数据共享属性的分类，禁止擅自增设条件阻碍、影响政务数据共享。**三是**细化共享使用要求。规定通过共享获取政务

数据能够满足履职需要的，政府部门不得重复收集，明确牵头收集政务数据的政府部门的职责。细化政务数据共享申请、答复流程及时限要求。明确政务数据质量管理、校核纠错及共享争议解决处理机制。规定上级政府部门应当根据下级政府部门的履职需要，在确保政务数据安全的前提下，及时、完整回流相关政务数据。**四是**加强平台支撑。规定整合构建全国一体化政务大数据体系，要求已建设的政务数据平台纳入全国一体化政务大数据体系，原则上不新建政务数据共享交换系统。明确各级政府部门应当通过全国一体化政务大数据体系开展政务数据共享工作。**五是**强化保障措施。按照谁管理谁负责、谁使用谁负责的原则，明确各环节安全责任主体，强调需求部门在使用依法共享政务数据过程中的安全管理责任。细化政府部门和受托方政务数据安全保护义务，明确个人信息保护及处理投诉举报要求。提出政务数据共享经费保障和预算管理要求。该《条例》的出台，填补了我国在政务数据共享领域的立法空白，对于健全政务数据管理法律体系，实现政务数据共享工作法治化、规范化具有重要的引领和推进作用。

2.密集推出数据资源开发利用规范性文件

《全国数据资源调查报告（2024 年）》显示，我国数据资源规模优势持续扩大，数据资源开发利用活跃度稳步提升，各类主体加快人工智能布局投入，数据要素市场化、价值化进程进一步提速，然而，我国仍存在数据资源区域和行业分布不均衡的问题。2025 年，我国通过密集出台相关规范文件，明晰数据流通安全治理机制、规范公共数据资源授权运营等，进一步激发供数动力和用数活力。

完善数据流通安全治理机制。数据流通安全治理规则是数据基础制度的重要内容，是推动建设高水平数据市场的保障。1 月，国家发展改革委等部门印发《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》。该《方案》坚持系统思维、底线思维，将安全贯穿数据供给、流通、使用全过程，以成本最小化实现安全最优化，充分释放数据价值，促进数据开发利用。在主要任务方面，《方案》从明晰企业数据流通安全规则、加强公共数据流通安全管理、强化个人数据流通保障、完善数据流通安全责任界定机制、加强数据流通安全技术应用、丰富数据流通安全服务供给、防范数据滥用风险等七个方面作出具体部署。

初步形成公共数据资源开发利用“1+3”政策体系。《中共中央办公厅 国务院办公厅关于加快公共数据资源开发利用的意见》明确要求建立公共数据资源登记制度，鼓励探索公共数据资源授权运营，建立健全价格形成机制。作为落实《意见》要求的重要举措，1 月，国家发展改革委、国家数据局公布了《公共数据资源登记管理暂行办法》《公共数据资源授权运营实施规范（试行）》《关于建立公共数据资源授权运营价格形成机制的通知》三份政策文件，对公共数据资源开发利用特别是授权运营全流程进行指导和规范，标志着公共数据资源开发利用“1+3”政策体系初步形成。其中，《公共数据资源登记管理暂行办法》明确了公共数据资源登记的基本要求，形成全国一体化的公共数据资源登记体系，为建立公共数据资源底账、提高公共数据资源可用性奠定基础。《公共数据资源授权运营实施规范（试行）》着

眼建立国家层面统一的制度环境，明确授权运营应把握的主要原则和实施路径，是推动公共数据资源价值有序释放的重要保障，为规范化开展公共数据资源授权运营提供指引。《关于建立公共数据资源授权运营价格形成机制的通知》基于公共数据资源授权运营机制的特点，旨在通过建立符合公共数据要素特性的价格形成机制，更好促进公共数据资源运营机构健康规范发展。

细化数据资源统计和数据流通交易相关规则。2 月，国家数据局综合司、公安部办公厅印发《全国数据资源统计调查制度》，构建了覆盖公共数据、科学数据、企业数据 3 个领域和 12 张报表的统计调查报表体系。该《调查制度》的印发标志着全国数据资源统计调查工作正式迈入制度化规范化新阶段，有助于摸清全国数据资源底数，准确、及时、全面反映我国数据资源全貌。7 月，国家数据局、国家市场监管总局联合印发了《数据提供合同（示范文本）》《数据委托处理服务合同（示范文本）》《数据融合开发合同（示范文本）》《数据中介服务合同（示范文本）》。示范文本聚焦数据流通中最典型的 4 类场景，约定了数据产权安排、安全保密要求、违约责任、争议解决等通用条款，并围绕数据流通交易各方权利义务、数据情况、数据交付和验收标准等进行了针对性和差异化安排。示范文本以标准化形式引导经营主体在合同中约定责任边界，有助于降低数据流通交易成本、维护公平竞争环境、推动数据市场健康有序发展。

3.持续深化个人信息保护和数据安全管理制度

落实个人信息保护相关制度。《个人信息保护法》对个人信息保护合规审计、大型网络平台个人信息保护特别义务等作出明确规定。2025 年，我国持续完善个人信息保护制度，不断推动《个人信息保护法》落地实施。**一是**细化个人信息保护合规审计操作规范。个人信息保护合规审计是监督与评估个人信息处理者切实履行个人信息保护义务的重要制度。为有效落实《个人信息保护法》第五十四条的相关要求，2 月，国家互联网信息办公室公布《个人信息保护合规审计管理办法》。该办法对合规审计活动的开展、合规审计机构的选择、合规审计的频次、个人信息处理者和专业机构在合规审计中的义务等作出细化规定，旨在为个人信息处理者开展个人信息保护合规审计提供系统性、针对性、可操作性的规范，提升个人信息处理活动合法合规水平，保护个人信息权益。**二是**健全企业个人信息保护监督委员会制度。为落实《个人信息保护法》第五十八条规定，指导规范大型网络平台设立、运行个人信息保护监督委员会，对个人信息保护情况进行监督，保护个人信息权益，9 月，国家互联网信息办公室公布《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》，对个人信息保护监督委员会的组成、任职要求等进行了细化。**三是**规范大型网络平台个人信息处理活动。大型网络平台作为个人信息处理的核心载体，是数字经济时代人们生产生活的重要场所，也是个人信息保护的关键环节。11 月，国家互联网信息办公室、公安部发布《大型网络平台个人信息保护规定（征求意见稿）》，明确大型网络平台

目录管理制度，要求大型网络平台服务提供者指定个人信息保护负责人、明确个人信息保护工作机构，细化个人信息可携权相关规则，有助于进一步保护个人信息合法权益、促进平台经济健康发展。

细化明确重点领域数据安全合规底线要求。我国在《数据安全法》的基础上，通过出台一系列规章文件进一步明确了工业和信息化、自然资源、会计师事务所、银行保险机构等相关领域数据安全管理要求。2025 年，为进一步夯实数据安全的法治基础，我国加快推动中国人民银行业务领域、能源行业等行业领域数据安全管理的法治化建设。5 月，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，对中国人民银行业务领域数据分类分级与总体要求、全流程业务数据安全管理要求、全流程业务数据安全技术要求、业务数据安全风险与事件管理等方面作出规定。12 月，国家能源局印发《能源行业数据安全管理办法（试行）》，明确了国家能源主管部门、省级能源主管部门、能源数据处理者的基本职责和权利义务，对能源行业重要数据、核心数据的精准识别和安全保护提出了明确要求。

表 1 重点行业领域数据安全管理相关规定

日期	文件名称
2021.08	《汽车数据安全管理若干规定（试行）》
2022.12	《工业和信息化领域数据安全管理办法（试行）》
2024.03	《自然资源领域数据安全管理办法》
2024.04	《会计师事务所数据安全管理暂行办法》
2024.12	《银行保险机构数据安全管理办法》
2025.05	《中国人民银行业务领域数据安全管理办法》
2025.12	《能源行业数据安全管理办法（试行）》

规范公共安全视频系统管理。随着我国经济社会发展和公众安全需求日益提高，公共安全视频图像信息系统被广泛应用在社会管理各个领域。但同时，也存在建设管理不规范、信息安全与个人隐私保护隐患等社会关注、反响强烈的问题。1 月，国务院公布《公共安全视频图像信息系统管理条例》，旨在规范公共安全视频系统管理，维护公共安全，保护个人隐私和个人信息权益。该条例加大保护力度，确保个人信息安全，明确对保存期限届满后已实现处理目的的视频图像信息应当予以删除，严格规范国家机关、个人查阅调取视频图像信息的权限、程序，要求公开传播视频图像信息时严格保护个人、组织相关信息，明确在非公共场所安装图像采集设备设施不得危害公共安全或者侵犯他人合法权益。

进一步规范国家网络身份认证公共服务建设。国家网络身份认证公共服务有助于满足人民群众在数字化、网络化、智能化条件下安全、便捷证明个人身份的需求。为规范国家网络身份认证公共服务平台的运行管理，保护用户个人信息权益，5 月，公安部、国家互联网信息办公室等六部门联合公布《国家网络身份认证公共服务管理办法》。该办法一是明确了国家网络身份认证公共服务及网号、网证的概念、申领方式；二是明确了使用国家网络身份认证公共服务的效力、应用场景；三是强调了国家网络身份认证公共服务平台、互联网平台等对数据安全和个人信息保护的责任；四是对未成年人申领、使用国家网络身份认证公共服务作出特殊规定。

4.不断推动数据出境安全管理政策落地见效

我国积极促进数据依法有序自由流动，通过《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息保护认证实施规则》《促进和规范数据跨境流动规定》等法律文件，构建形成了以重要数据和个人信息为两大类出境数据，以数据出境安全评估、个人信息出境标准合同、个人信息保护认证为主要数据出境路径的数据跨境流动制度。2025 年，我国持续完善高效便利安全的数据出境安全管理体系，不断深化实施数据出境负面清单制度，明确典型业务场景下数据出境的具体要求和便利化举措。

持续优化数据出境管理政策。一是完善个人信息保护认证数据出境路径。《个人信息保护法》明确了个人信息保护认证作为个人信息出境的合法机制之一，《关于实施个人信息保护认证的公告》《个人信息保护认证实施规则》规定了个人信息保护认证的认证依据、模式与流程。为进一步细化个人信息保护认证制度的具体要求，10 月，国家互联网信息办公室、国家市场监督管理总局联合公布《个人信息出境认证办法》，对个人信息出境认证的适用情形、申请方式、认证要求及证书有效期，专业认证机构应当履行的义务，监督管理要求等作出细化规定。该办法的出台标志着《个人信息保护法》明确的数据出境安全评估、个人信息保护认证、个人信息出境标准合同等出境制度设计的全面落地，也标志着我国数据跨境流动制度体系的全面建立。**二是**细化重点行业数据出境规则。2025 年，相关行业主管部门逐步

细化明确具体行业领域的数据出境业务场景规则以及个人信息出境必要范围。4 月，中国人民银行等六部门联合印发《促进和规范金融业数据跨境流动合规指南》，进一步明确数据出境的具体情形以及可跨境流动的数据项清单，并要求金融机构采取必要的数据安全保护管理和技术措施切实保障数据安全。6 月，工业和信息化部等八部门发布《汽车数据出境安全指引（2025 版）（征求意见稿）》，拟进一步细化重要数据出境、数据出境实施流程以及汽车数据出境安全保护等方面具体要求。

多地发布自贸试验区数据出境负面清单。《促进和规范数据跨境流动规定》建立自贸试验区数据出境负面清单制度，鼓励自贸试验区结合实际制定数据出境负面清单，成为促进和便利自贸试验区数据跨境流动的一项创新举措。2025 年，上海、海南、浙江、重庆、江苏、广西等地发布自贸试验区（港）数据出境负面清单，推动实现高效便捷数据出境，数据出境负面清单制度实施初见成效。

5.着力加强数据权益司法保护

首次发布数据权益司法保护专题指导性案例。数据具有十分复杂的经济和法律特征，给传统法律制度带来新挑战。对于因数据权属、流通交易、收益分配、安全保障等问题引发的矛盾纠纷，需要人民法院通过司法裁判不断探索科学合理的保护路径。2 月，中共中央印发《关于加强新时代审判工作的意见》，要求人民法院“依法审理数据产权归属认定、市场交易、权益分配、利益保护等纠纷，推动数据要素高效流通和交易”。8 月，最高人民法院发布第 47 批指导性案例

（指导性案例 262—267 号），这是最高人民法院首次发布数据权益司法保护专题指导性案例，涵括不正当竞争纠纷、侵权责任纠纷、个人信息保护纠纷、执行实施等涉数据权益案件多发案由类型，涉及数据权属认定、数据产品利用、个人信息保护、网络平台账号交付等社会高度关注的问题。该批案例是专题指导性案例，效力位阶较高，各级人民法院审判类似案件时应当参照，且在裁判文书中的裁判理由部分可以引述相关指导性案例，对于统一类案裁判尺度、充分发挥司法在数据基础制度建设中的作用具有积极意义。

探索网络不正当竞争纠纷中的数据权益分配规则。在网络不正当竞争纠纷中，数据权益的分配是核心争议点之一，其本质是在数据来源者、平台经营者、数据加工者以及社会公众之间寻求公平与效率的平衡。为了解决这些争议并为市场提供明确预期，我国司法实践不断探索和明确规则。最高人民法院发布的第 47 批指导性案例中，对“数据爬取是否合法”“跨平台数据转移能否允许”等争议作出回应，明确法律适用、统一裁判标准，为企业数据竞争划定清晰边界。**一是**禁止“实质性替代”的恶意数据爬取。明确对于未经许可获取并向公众提供相关数据，实质性替代网络平台产品或者服务，扰乱市场竞争秩序、损害网络平台经营者或者其他权利人合法权益的行为，人民法院可以适用《反不正当竞争法》有关规定，认定构成不正当竞争行为。**二是**允许基于“用户授权”的合规数据转移。网络平台向用户提供关联账号服务，经用户授权后转移其在关联网络平台获取的数据，为用户在合理范围内处理该数据提供便利，未扰乱市场竞争秩序的，不构

成不正当竞争行为。7 月，上海市高级人民法院作出网络不正当竞争纠纷中的数据权益分配应遵循贡献比例原则的民事判决。法院基于金融市场对数据流通性的客观需要，判定对此类数据权益可遵循贡献比例原则予以综合认定，即对数据的生成作出贡献的主体，可按其实际投入比例享有相应权益。在具体案件中，需基于现有法律框架和法律基本原则，结合数据类型、应用场景、生成过程、贡献程度、双方约定、利益平衡等不同因素对相关数据权益的分配予以综合认定。

专栏 1 最高人民法院发布指导性案例 探索数据不正当竞争纠纷裁判规则

在涉数据权益民事审判中，不正当竞争纠纷案件较为集中。最高人民法院在发布的数据权益司法保护专题指导性案例中，选取了《某科技有限公司诉某文化传媒有限公司不正当竞争纠纷案》（指导性案例 262 号）和《某网络信息技术有限公司诉某信息科技有限公司不正当竞争纠纷案》（指导性案例 263 号）两个涉不正当竞争纠纷的案例，以“一正一反”对照模式，编制形成数据不正当竞争纠纷的裁判规则体系。

指导性案例 262 号是一件因爬取搬运网络平台数据而引发的不正当竞争纠纷案件。该案中，某文化公司运营的乙APP未经许可，抓取、搬运某科技公司甲APP内大量短视频、用户信息及评论，导致乙APP与甲APP内容高度同质化，实质性替代甲APP的产品和服务。该案认定某文化公司未经许可获取并向公众提供相关数据，足以实质性替代某科技公司提供的产品和服务，构成不正当竞争行为。

指导性案例 263 号是一件涉网络平台关联账号服务的不正当竞争纠纷案件。该案中，某网络公司运营的甲网站为求职者与招聘企业提供服务，某信息公司运营的乙网站设有“关联外网账号”功能。招聘企业用户在甲网站获取的个人简历，在使用“关联外网账号”功能后可以在乙网站中搜索到。该案例针对关联账号服务这一网络空间中较为常见的服务模式，认为网络用户使用关联账号功能，将其持有的数据在不同网络平台间转移，系合法正当行为。

上述两个涉不正当竞争纠纷的案例遵循“数据二十条”有关“统筹发展和安全”、“把该管的管住、该放的放开”精神，引导市场主体对数据“取之有道、用之

有度”。一方面，为爬取搬运网络数据行为划定了“红线”，推动数据要素收益向数据价值和使用价值创造者合理倾斜；另一方面，最大限度地保障数据来源者在参与网络经济活动中的自主选择权，对于促进数据共享共用，增强数据要素共享性、普惠性，释放数据价值红利，推动数字经济发展具有重要意义。

（二）新技术新应用立法加速推进，人工智能治理实践日渐丰富

1.逐步健全人工智能制度体系

构建人工智能生成合成风险“技治+法治”双重防线。随着人工智能技术快速发展，生成合成技术滥用、虚假信息传播扩散加剧等问题引发社会各界的关切。3 月，国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局联合发布《人工智能生成合成内容标识办法》。该办法以内容标识为抓手，细化前期相关部门规章的标识相关要求，明确相关服务主体的标识责任义务，规范内容制作、传播各环节标识行为。该办法明确人工智能生成合成内容标识主要包括显式标识和隐式标识两种形式，强调任何组织和个人不得恶意删除、篡改、伪造、隐匿办法规定的生成合成内容标识，不得为他人实施上述恶意行为提供工具或者服务。与此同时，强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》支撑该办法的实施，对人工智能生成合成内容服务提供者与网络信息传播服务提供者提出了内容标识方法的具体要求。两者同步推出、同步实施，对相关主体规范开展标识活动提供了详细指导。

细化人工智能领域科技伦理管理规则。人工智能应用伴随产生的伦理问题是全世界面临的共同挑战。促进智能向善，需要加强科技伦理治理，强化科技伦理审查作用。《关于加强科技伦理治理的意见》对“强化科技伦理审查和监管”作出部署，《科技伦理审查办法（试行）》对科技伦理审查的基本程序、标准、条件等提出统一要求。作为科技伦理管理在人工智能领域的具体落实，8 月，工业和信息化部发布了《人工智能科技伦理管理服务办法（试行）（公开征求意见稿）》。该征求意见稿**一是**提出了人工智能科技伦理支持与促进措施，从标准建设、服务体系、鼓励创新等方面提出相关举措；**二是**明确了人工智能科技伦理管理的实施主体，为从事人工智能相关活动的高等学校、科研机构、医疗卫生机构、企业等提供指引；**三是**明确了人工智能科技伦理管理的申请与受理、一般程序与简易程序、专家复核程序、应急程序等工作程序，并提出了需要开展科技伦理专家复核的人工智能科技活动清单。

明确人脸识别技术应用安全边界。人脸识别技术应用与人脸信息安全紧密相关，在促进数字经济发展、方便人民生活的同时，也引发了公众对侵犯隐私、泄露个人信息的担忧。3 月，国家互联网信息办公室、公安部联合公布《人脸识别技术应用安全管理办法》。该办法**一是**明确应用人脸识别技术处理人脸信息的基本要求；**二是**明确应用人脸识别技术处理人脸信息的处理规则，规定应用人脸识别技术处理人脸信息，应当具有特定的目的和充分的必要性，个人信息处理者应当履行告知、进行个人信息保护影响评估等义务；**三是**明确人脸识别

技术应用安全规范，规定实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，不得将人脸识别技术作为唯一验证方式，明确在公共场所安装人脸识别设备的具体要求；**四是**明确监督管理职责和法律责任，规定了人脸识别技术应用备案相关要求。

出台人工智能细分领域应用服务规则。4 月，中国气象局、国家互联网信息办公室发布部门联合规章《人工智能气象应用服务办法》。作为世界气象组织会员中首部关于人工智能气象应用服务的法律规范，该办法围绕数据开放、算法模型研发和应用场景赋能等提出了具体政策支持和促进措施，加强人工智能与气象监测预警、预报预测、数值预报等领域深度融合应用，构建人工智能气象应用服务场景。同时对气象主管机构参与国际气象领域人工智能应用服务的发展和治理做出了规定。10 月，中央网信办、国家发展改革委联合印发《政务领域人工智能大模型部署应用指引》。作为我国首个公开面向政务领域大模型应用的专项政策文件，该指引围绕总体要求、应用场景、规范部署、运行管理、保障措施等方面提出了一系列要求举措，标志着我国政务领域人工智能大模型应用迈入有序推进新阶段。12 月，国家互联网信息办公室发布《人工智能拟人化互动服务管理暂行办法（征求意见稿）》，拟促进人工智能拟人化互动服务健康发展和规范应用。

2.探索构建卫星互联网制度规范

制定政策文件促进卫星通信产业高质量发展。卫星互联网作为未来通信网络的重要组成部分，是构建空天地海一体化通信系统、实现

全球万物互联的基础，其战略价值日益凸显。为提升卫星网络国内协调效率，优化协调程序，促进卫星频率轨道资源高效开发利用，维护空中电波秩序，3 月，工业和信息化部印发《卫星网络国内协调管理办法（暂行）》，从卫星网络国内协调关系的建立、国内协调的开展、国内协调的完成等方面进行了规定，对于解决国内协调难题、减轻企业负担、促进商业航天发展具有重要意义。8 月，工业和信息化部印发《关于优化业务准入促进卫星通信产业发展的指导意见》，围绕促进卫星通信产业高质量发展，从有序扩大市场开放、持续拓展应用场景、培育壮大产业生态、优化电信资源供给、加强卫星通信监管、提升协同推进合力等六方面提出 19 条思路举措。

出台规定促进和规范终端设备直连卫星服务健康发展。近年来，终端设备直连卫星已成为全球移动通信领域发展热点和趋势，产品和服务加快普及。与此同时，技术滥用也对传统网络管理方式带来新挑战，可能引发网络安全风险、数据安全风险、个人信息保护风险和电信网络诈骗风险等。4 月，国家互联网信息办公室、国家发展改革委、工业和信息化部、公安部、海关总署、市场监管总局、广电总局联合发布《终端设备直连卫星服务管理规定》，为终端设备直连卫星服务管理工作提供了具体指引。**一是**明确制定目的是促进和规范终端设备直连卫星服务健康发展。**二是**明确对终端设备直连卫星技术研发、基础设施建设、融合创新、应用生态、标准研制、人才培养等方面的支持措施。**三是**强调向境内提供终端设备直连卫星服务等应依照《电信条例》《无线电管理条例》取得相关许可和核准，提供相关服务应履

行网络安全、数据安全、违法信息处置等方面的义务。**四是**明确有关部门依据职责依法开展监督管理。

3.探索构建电子单证应用相关规定

随着区块链、大数据等技术在航运领域的广泛应用，电子提单、电子运单等数字化单证日益普及。为了促进和规范电子单证推广应用，提高货物贸易和运输数字化水平，降低全社会物流成本，保障电子单证活动当事人合法权益，维护国家安全和社会公共利益，9 月，国家互联网信息办公室发布《促进和规范电子单证应用规定（征求意见稿）》，从电子单证应用的促进和电子单证系统的可靠性、安全性等方面，对电子单证应用的创新发展与风险防范作出规定。10 月，十四届全国人大常委会第十八次会议表决通过修订后的《海商法》。本次修订适应航运单证电子化不断发展的实践需求，参考借鉴《联合国贸易法委员会电子可转让记录示范法》和有关国际公约，在第四章“海上货物运输合同”中专节规定电子运输记录，明确电子运输记录的法律地位，规定符合法定条件的电子运输记录与运输单证具有同等效力。

4.不断加强人工智能执法司法应对

人工智能执法监督深入开展。随着人工智能技术的快速发展和广泛应用，滥用人工智能技术从事违法犯罪的活动日益增多，对社会秩序和公众合法权益造成了威胁。我国综合运用专项行动、行政执法、服务备案等多种手段，实现引导发展与防范风险的双重目标。**一是**持续开展生成式人工智能服务备案工作。截至 2025 年 11 月 1 日，累计有 611 款生成式人工智能服务完成备案，306 款生成式人工智能应用

或功能完成登记。**二是**开展专项行动整治人工智能技术滥用乱象。4月，中央网信办部署开展“清朗·整治AI技术滥用”专项行动。第一阶段强化AI技术源头治理，第二阶段聚焦利用AI技术制作发布谣言、不实信息、色情低俗内容，假冒他人、从事网络水军活动等突出问题。在第一阶段的工作中，累计处置违规小程序、应用程序、智能体等AI产品 3500 余款，清理违法违规信息 96 万余条，处置账号 3700 余个，各项工作取得积极进展。**三是**依法压实人工智能服务提供者安全主体责任。7 月，工业和信息化部办公厅印发《工业和信息化部行政执法事项清单（2025 年版）》，明确了对生成式人工智能服务提供者落实安全主体责任的监督检查；对工业和信息化领域提供生成式人工智能服务的网络数据处理者未加强对训练数据及其处理活动的安全管理，未采取有效措施防范处置网络数据安全风险的行政处罚；对生成式人工智能服务提供者未履行落实安全主体责任的行政处罚等行政执法事项。10 月，工业和信息化部通报了 20 款存在侵害用户权益行为的智能终端，其中包括多款智能音箱、智能门锁、智能学习终端产品等。

人工智能司法实践日渐丰富。人工智能技术加速发展，新领域、新业态、新模式不断涌现，各种新型矛盾纠纷也相伴而生。2025 年，面对人工智能引发的新型、疑难、复杂案件，我国持续开展涉人工智能纠纷案件的审理工作，涵盖知识产权侵权、不正当竞争等多个案由。**一是**人工智能生成物的可版权性。人工智能生成物的可版权性及权利归属相关问题，成为了人工智能产业发展需要直面解决的核心法律问

题之一。此前，北京、江苏等地法院已作出认可人工智能生成物版权性的判决。2025 年，相关著作权侵权尤其是“AI文生图”纠纷数量不断增加，同时也出现了因无法提供创作过程记录而不认可人工智能生成物构成作品的判决。**二是**涉及人工智能不正当竞争相关案件。在人工智能模型结构和参数的反不正当竞争法保护方面，3 月，北京知识产权法院二审审结全国首例案件，明确模型的结构和参数可以构成受《反不正当竞争法》保护的竞争利益，认为未经许可直接使用他人通过数据训练获得的模型结构和参数的行为违反了人工智能模型领域公认的商业道德，具有不正当性。在人工智能服务的不正当竞争方面，8 月，浙江省杭州市中级人民法院就涉生成式人工智能服务不正当竞争纠纷案作出二审判决，认定通过人工智能写作工具提供“种草文案”等服务构成不正当竞争，明确以特定场景为应用层提供生成式人工智能服务，理应尊重该特定应用场景的规则，并结合其应用场景、行为目的、行为方式等方面合理设定生成式人工智能服务提供者的注意义务，避免人工智能服务成为实施侵权行为的工具。

专栏 2 全国首例保护人工智能模型结构和参数生效判决
变身漫画特效模型（包括结构与参数）系由A公司基于基础模型利用手绘师绘制的漫画数据与相对应的真人数据予以训练，并不断调整模型结构与参数得来。该模型被用于A公司经营的甲应用程序中的变身漫画特效功能，可以将用户实时拍摄的照片、视频转换为漫画风格。B公司运营的乙应用程序在后上线了少女漫画特效功能，同样可实现漫画风格的实时转换。A公司认为B公司的少女漫画特效模型与其变身漫画特效模型在结构、参数等方面存在高度的相似性，构成侵权，请求判令停止侵权并赔偿损失。 北京市朝阳区人民法院一审判决认定，B公司通过使用与变身漫画特效高度

相似的模型使少女漫画特效能够起到替代变身漫画特效的效果，损害了A公司竞争利益，构成不正当竞争。北京知识产权法院二审维持原判。

本案的典型意义在于明确了人工智能模型结构和参数的可保护性，并根据在案情形探索了一种基于竞争利益的保护路径。在本案中，法院认可通过数据训练获得的模型结构和参数构成受到反不正当竞争法保护的竞争利益，并明确未经许可直接使用他人通过数据训练获得的模型结构和参数的行为违反了人工智能模型领域公认的商业道德。同时，该行为还扰乱市场竞争秩序并损害消费者长远利益，具有不正当性。

（三）网络生态治理体系持续优化，平台经济监管制度不断健全

1.着力破解网络生态治理突出问题

深化“自媒体”及MCN机构治理。我国针对自媒体和MCN机构乱象、网上“饭圈”乱象、热搜榜单乱象等网络空间的突出问题，不断完善垂直细分领域法律法规，持续开展专项整治。**一是**规范MCN机构互联网信息内容相关业务活动。1 月，国家互联网信息办公室起草发布《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》，拟对境内运营的网络信息内容多渠道分发服务机构开展互联网信息内容相关业务活动进行规定。**二是**规范“自媒体”医疗科普行为。7 月，中央网信办秘书局、国家卫生健康委办公厅、市场监管总局办公厅、国家中医药管理局综合司联合印发《关于规范“自媒体”医疗科普行为的通知》，规范“自媒体”医疗科普信息发布传播行为，防范虚假医疗科普信息误导公众，维护人民群众合法权益。**三是**开展“自媒体”相关专项整治行动。7 月，中央网信办秘书局发布关于开展“清朗·整治‘自媒体’发布不实信息”专项行动的通知。本次专项行动重点

整治恶意蹭炒误导公众问题、多种手段歪曲事实问题、不做标注以假乱真问题、专业领域信息不实问题四类突出问题。

细化军事、宗教等重点领域管理规范。一方面，加强互联网军事信息传播管理。1 月，国家互联网信息办公室、工业和信息化部、公安部、国家安全部、文化和旅游部、国家广播电视总局、国家国防科技工业局、国家保密局、中央军委政治工作部、中央军委政法委员会联合印发《互联网军事信息传播管理办法》。该办法为开办军事网站平台、网站平台军事栏目和军事账号提供规范指引，规定了军事账号的认定和核验报送要求，明确了互联网军事信息传播的具体要求，并对建立互联网军事信息传播管理工作协调机制作出具体安排。**另一方面，**明确宗教教职人员网络行为规范。9 月，国家宗教事务局印发《宗教教职人员网络行为规范》，明确宗教教职人员实施网络行为的基本原则与具体要求；规定宗教教职人员在互联网上讲经讲道或者从事宗教教育培训，可以且仅限于通过取得《互联网宗教信息服务许可证》的宗教团体、宗教院校、寺观教堂依法自建的互联网站、应用程序、论坛等进行。

2.切实维护特殊群体网络空间合法权益

进一步细化未成年人网络保护制度。6 月，国家互联网信息办公室发布《可能影响未成年人身心健康的网络信息分类办法（征求意见稿）》。该办法作为配套文件，主要是细化《未成年人网络保护条例》第二十三条可能影响未成年人身心健康的信息的具体种类、范围、判断标准和提示办法，进一步健全完善未成年人网络保护制度，营造有

利于未成年人身心健康的网络环境。9 月，国家互联网信息办公室发布《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》。该办法落实《未成年人网络保护条例》相关制度要求，细化了具体认定标准、认定流程和相关工作要求，压紧压实网络平台未成年人网络保护主体责任。

3.规范引导网络平台合规运营

优化平台经济竞争生态。互联网平台网络效应明显，涉及平台经营者、平台内经营者、消费者和从业人员等多方主体。平台经营者具有一定的管理者属性，通过平台规则、数据、算法、技术手段等影响平台竞争生态，一旦从事排除、限制竞争行为，将会损害多方主体利益。6 月，十四届全国人大常委会第十六次会议表决通过新修订的《反不正当竞争法》。本次修订直面网络不正当竞争行为新情况新问题，进一步完善数字经济领域公平竞争规则。**一是**加大对平台不正当竞争行为监管力度，规定平台经营者不得强制或者变相强制平台内经营者按照其定价规则，以低于成本的价格销售商品，扰乱市场竞争秩序。**二是**合理设置平台经营者义务，规定平台经营者应当在平台服务协议和交易规则中明确平台内公平竞争规则，并对平台经营者处置平台内经营者不正当竞争行为作出规定。**三是**对侵害数据权益、恶意交易等不正当竞争行为作出规定。11 月，市场监管总局发布《互联网平台反垄断合规指引（征求意见稿）》。该指引根据《反垄断法》等法律规定，在充分总结近年来我国平台反垄断执法经验的基础上，明确平台经营者加强反垄断合规管理的基本原则，细化风险识别的考量因素

和风险管控的具体措施，为平台经营者落实落细合规主体责任提供明确、清晰的指引，对于有效预防和化解垄断风险、促进平台经济规范健康发展具有重要意义。

针对性地规范直播电商行业。直播电商行业在快速发展的同时，虚假营销、假冒伪劣等乱象逐渐显现，损害了广大消费者合法权益，影响了直播电商行业规范健康发展。6 月，市场监管总局公布《直播电商监督管理办法（征求意见稿）》，细化直播电商平台经营者的责任和义务，明确直播间运营者、直播营销人员服务机构、直播营销人员的责任义务，规定直播电商活动的管辖适用、协同监管、监督检查、信用监管、约谈与整改等内容。8 月，市场监管总局发布《直播电商落实食品安全主体责任监督管理规定（征求意见稿）》，明确了从事食品经营活动的直播间运营者的准入要求，明确了直播电商平台经营者在建立档案、培训人员、信息保存公示等方面的责任，明确了直播间运营者、直播营销人员服务机构和直播营销人员责任。

细化平台经济领域价格行为规定。平台经济领域涉及的经营者众多，其价格行为关系消费者切身利益。然而，当前一些行业低价无序竞争问题凸显，对价格调控监管提出新要求。7 月，《价格法修正草案（征求意见稿）》公开征求意见，完善低价倾销的认定标准，规范市场价格秩序，治理“内卷式”竞争。同月，市场监管总局发布《网络交易平台收费行为合规指南》，进一步规范网络交易平台向平台内经营者收取佣金、抽成、会员费、技术服务费、信息服务费、营销推广费等收费行为。9 月，国家发展改革委、市场监管总局印发《关于治

理价格无序竞争 维护良好市场价格秩序的公告》，聚焦价格无序竞争对行业发展、产品创新、质量安全等造成的负面影响，在保护经营者自主定价权的前提下，按照事前引导和事中事后监管相结合的思路，采取调研评估行业平均成本、加强价格监管、规范招标投标行为等措施，维护公平竞争市场环境。12 月，国家发展改革委、市场监管总局、国家网信办联合印发《互联网平台价格行为规则》，在现行规定的基础上，结合平台经济领域价格行为特点，细化相关监管要求，从引导经营者依法自主定价、规范价格标示和价格竞争行为等方面，为经营者提供明确的行为指引。

规制外卖平台服务管理行为。今年以来，外卖平台企业为争夺即时零售流量入口，反复发起“百亿补贴”“大额神券”等外卖大额补贴活动，“外卖大战”一定程度上加剧了餐饮市场“内卷”。7 月，市场监管总局约谈相关平台企业，要求企业进一步规范促销行为，理性参与竞争，共同构建消费者、商家、外卖骑手和平台企业等多方共赢的良好生态，促进餐饮服务行业规范健康持续发展。12 月，市场监管总局批准发布了推荐性国家标准《外卖平台服务管理基本要求》，针对外卖行业出现“幽灵外卖”、非理性竞争以及配送员相关权益保障不足等问题，通过标准化工作细化法律法规的要求，引导行业健康有序发展。

规范平台相关数据和信息的报送。3 月，市场监管总局印发《网络交易合规数据报送管理暂行办法》，规定了网络交易合规数据报送范围、报送时限、报送层级，网络交易合规数据利用和管理等内容，

对推动网络交易平台经营者落实数据报送主体责任，依法合规经营，发挥数据在平台经济治理中的关键要素作用，探索开展穿透式监管，提升网络交易监管效能具有积极意义。6 月，国务院公布《互联网平台企业涉税信息报送规定》，明确了报送义务、内容和时限要求，规定了免予报送的情形、减轻报送负担的措施、涉税信息的保密义务等。该规定的出台对于健全平台经济治理机制，规范平台经济税收秩序，促进平台经济规范健康持续发展具有重要意义。

4.营造民营经济发展良好环境

出台民营经济发展基础性法律，保护民营经济组织和经营者合法权益。4 月，第十四届全国人民代表大会常务委员会第十五次会议通过《民营经济促进法》。该法共 9 章 78 条，围绕公平竞争、投资融资促进、科技创新、规范经营、服务保障、权益保护等方面建立完善相关制度机制，将党中央对民营经济平等对待、平等保护的要求落下来，持续优化稳定、公平、透明、可预期的民营经济发展环境。该法强调保护民营经济组织和经营者的人格权益，规定任何单位和个人不得利用互联网等传播渠道，以侮辱、诽谤等方式恶意侵害民营经济组织及其经营者的人格权益。该法对网络服务提供者赋予法定义务：即建立健全投诉、举报机制，及时处置恶意侵害当事人合法权益的违法信息并向有关主管部门报告。

整治涉企网络“黑嘴”，进一步优化营商网络环境。当前网络上出现的恶意抹黑企业、敲诈勒索、恶意营销炒作和泄密侵权等行为损害民营企业声誉和利益，扰乱市场秩序。为落实中央经济工作会议精神、

《民营经济促进法》有关要求，5 月，中央网信办开展“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动，聚焦网络“黑嘴”伤企乱象，重点整治恶意抹黑诋毁攻击企业问题、对企业进行敲诈勒索问题、恶意营销炒作问题、泄密侵权类问题四类突出问题，着力维护企业和企业家网络合法权益，护航经济高质量发展。在该专项行动的基础上，7 月与 9 月，国家网信办分别公开曝光两批典型案例，针对编造涉企虚假不实信息、发布涉企负面信息、蹭炒涉企热点等现象，督促网站平台强化涉企信息内容管理，依法依约处置一批涉企违法违规账号。

（四）网络安全法律体系不断完善，以高水平安全守护高质量发展

1.修改《网络安全法》

近年来，信息技术日新月异，网络应用更加普及，日益融入社会生产生活。与此同时，网络安全风险进一步凸显，利用网络从事网络入侵、网络攻击、传播违法信息等违法行为屡有发生。为适应网络安全新形势新要求，回应人工智能等战略性技术取得的新发展，我国对《网络安全法》作出修改，重点强化网络安全法律责任，加强与相关法律的衔接协调。

10 月，十四届全国人大常委会第十八次会议表决通过《全国人民代表大会常务委员会关于修改〈中华人民共和国网络安全法〉的决定》，自 2026 年 1 月 1 日起施行。该决定共 14 条，坚持问题导向、体系化衔接、分类施策，进一步筑牢国家网络安全屏障。**一是**回应人工智能治理和促进发展的需要。本次修改增加一条关于人工智能安全

与发展的框架性规定，支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展；支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。**二是**进一步完善法律责任。在深入总结网络安全法实施经验的基础上，本次修改完善了不依法履行网络运行安全保护义务行为、不依法履行违法信息处置义务行为的法律责任，同时，在个人信息保护方面进一步加强与民法典和个人信息保护法的衔接。**三是**增设网络设备安全罚则。对销售或者提供不符合要求的网络关键设备和网络安全专用产品的行为，增加规定法律责任，有效保障网络领域供应链安全。**四是**明确规范柔性执法情形。此次修订新增第七十三条，衔接《行政处罚法》，明确从轻、减轻或者不予处罚的情形，充分体现了过罚相当、惩教结合的原则，引导违法主体主动纠错、消除危害，有利于提升执法的精准度和公信力，同时为中小企业创新提供容错空间，实现法律效果与社会效果的统一。

2.完善网络安全防护制度规范

细化关键信息基础设施商用密码使用管理要求。6 月，国家密码管理局、国家互联网信息办公室、公安部联合发布《关键信息基础设施商用密码使用管理规定》。该规定细化《密码法》《商用密码管理条例》关于关键信息基础设施商用密码使用管理的基础性、原则性要求，明确划分密码管理部门、网信部门、公安机关以及保护工作部门、运营者的职权义务，明确规划、建设、运行等各阶段的规范要求，明

确制度、人员、经费等方面的保障措施，将关键信息基础设施商用密码使用管理各方面、各环节的要求以法定形式固化下来。

明确网络安全事件报告具体要求。近年来，各类网络安全事件频发，影响范围和危害程度不断升级。《网络安全法》第二十五条明确，网络运营者应当在发生危害网络安全的事件时，按照规定向有关部门报告。从网络安全事件应急处置工作实践来看，发生网络安全事件后及时向有关部门报告，有利于及时处置网络安全事件，防止危害扩大或产生不良社会影响。9 月，国家互联网信息办公室发布《国家网络安全事件报告管理办法》。该办法作为专门规定，明确了网络安全事件报告的监管职责，网络运营者的报告义务，同时针对关键信息基础设施、中央和国家机关及直属单位，以及其他网络运营者，分别明确了网络安全事件报告的流程和时限要求。

加强网络安全标识管理。随着物联网设备、智能终端广泛普及，网络攻击手段不断升级，安全漏洞频发，对个人隐私和公共安全构成严重威胁。为提升产品的网络安全能力，加强消费者权益保护，维护网络安全和公共利益，11 月，国家互联网信息办公室、工业和信息化部发布了《网络安全标识管理办法》（征求意见稿）和《实施网络安全标识的产品目录（第一批）》（征求意见稿），拟鼓励产品生产者标注网络安全标识、鼓励消费者优先选用标注网络安全标识的产品，并拟明确网络安全标识的等级划分、基本内容、基本样式等内容。

（五）涉外网络法治建设逐步深化，国际合作交流机制不断完善

1.积极推进全球人工智能发展与治理

深化全球人工智能发展合作。7 月，工业和信息化部推动中国—金砖国家人工智能发展与合作中心，联合开放原子开源基金会、CSDN中国开发者网络、OSC开源中国、启智社区、魔乐社区、飞桨星河社区、书生开源社区、智源社区、龙蜥社区、鲸智社区，共同发布《国际人工智能开源合作倡议》，号召全球以开源为纽带，共商技术创新路线，共促技术成果赋能，共建开放包容社区，共享时代发展红利。9 月，我国在全球发展倡议高级别会议上提出《“人工智能+”国际合作倡议》。该倡议主张秉持人类命运共同体理念，推动人工智能技术与经济社会发展深度融合，加速打造新质生产力，实现高质量发展和高水平安全良性互动，确保包括全球南方在内世界各国人民普遍受益。倡议围绕人工智能赋能民生福祉、科技进步、产业应用、文化繁荣、人才培养等五大重点方向，呼吁各国结合自身国情积极推进“人工智能+”行动，本着相互尊重、互利共赢原则加强政策交流和务实合作。

持续搭建世界级人工智能合作交流平台。7 月，2025 世界人工智能大会暨人工智能全球治理高级别会议在上海开幕。会上我国阐明中方推进人工智能发展和治理的主张，倡议成立世界人工智能合作组织，搭建产学研交流与成果共享的合作平台。我国还发表《人工智能全球治理行动计划》，在广泛吸收各国有益经验基础上，提出 13 项切实

可行的具体行动，以促进发展应用和确保安全可控为目标，强调尊重主权和公平普惠原则，重视应对能源环境问题，呼吁开展国际合作和协同治理。11 月，2025 年世界互联网大会乌镇峰会围绕“共筑开放合作、安全普惠的数智未来—携手构建网络空间命运共同体”主题，总结构建网络空间命运共同体理念提出 10 年来取得的丰硕成果和生动实践。期间，世界互联网大会发布《为人类共同福祉构建全球人工智能安全与治理体系》报告，系统梳理了当前全球人工智能安全与治理体系的探索与实践、应解决的关键问题及其他领域的全球治理多边实践经验。

2.稳步推进数据跨境对外合作

开展多双边数字治理对话交流。我国积极开展多双边数字治理合作，按照对等互利原则，探索与有关国家和地区就数据跨境流动建立特殊制度性安排。7 月，中国国家互联网信息办公室与德国联邦数字化和国家现代化部围绕数据跨境流动、人工智能治理等议题广泛深入交换意见，一致同意深化中德数据跨境流动合作，拓展人工智能治理领域交流，并就继续开展相关机制性对话达成共识。同月，中欧数据跨境流动交流机制第二次会议在布鲁塞尔举行。会上，双方就中欧数据跨境流动相关议题进行了深入、务实、富有建设性的交流，并结合双方企业诉求，就坚持双向对等原则进一步发挥机制作用，推动规则联通等达成广泛共识。双方同意设立工作组，就中欧汽车领域数据跨境流动开展合作。

三、2025 年域外互联网法治发展情况

2025 年全球在人工智能、数据治理、网络安全和平台治理等领域的法治实践不断深化，人工智能立法进入竞争性治理新阶段，更注重在安全可控与创新包容间寻求平衡；数据治理精细化，共享利用规则制度化，个人信息保护规则场景化；网络安全制度聚焦新技术应用风险，重点行业规范升级；平台治理重点强化内容管理、未成年人保护、消费者权益维护及反不正当竞争等方面的主体责任。

（一）人工智能立法迈向新阶段，促进和保障创新成为重点

1.人工智能综合性立法稳步推进

2025 年全球人工智能治理格局正经历深刻范式转变，从早期以应对安全风险为主导的治理模式，转向以机遇把握与国家利益博弈为核心的竞争性治理框架。多个司法辖区结合自身法治及产业发展特点推进人工智能综合性立法。在已通过和拟议的立法中，原则式立法、促进型立法成为主要模式，关注发展与安全平衡、为创新发展留出空间成为重要趋势。

美国人工智能立法面临复杂分歧与博弈。5 月，美国众议院通过了被称为“大而美”的法案，禁止各州和地方在法案生效后的 10 年内限制或以其他方式监管人工智能模型、人工智能系统或自动化决策系统。虽然在随后的 7 月，美国参议院投票删除了该条款，但该法案的制定过程，体现出美国在人工智能监管机制、监管强度、监管范围等方面的内部分歧，以及在促进创新与保护消费者之间的艰难平衡，同

时也对全球人工智能立法和治理产生重要影响。

专栏 3 美国《大而美法案》人工智能监管条款的争议和分析

美国作为全球人工智能产业的领跑者十分重视人工智能创新发展，美国联邦政府和州政府在立法层面积极探索构建适应技术发展和安全保障的法律法规，但复杂的利益平衡需求使得立法整体呈现出“声量大、步子小”的特点。联邦层面，“去监管”的治理模式成为焦点。5 月，美众议院通过一项联邦预算和税收改革法案《大而美法案》，其中包含一项 10 年内禁止实施州级人工智能监管规则的条款。7 月，该条款在受到州政府、联邦国会议员、社会组织等反对后，最终在法案中被删除。州层面，美国各州政府在 2025 年积极推动人工智能相关立法，覆盖技术研发和应用，重点关注生成式人工智能透明度、自动决策、高风险人工智能应用等。针对前沿人工智能模型，纽约州议会 6 月通过《负责任人工智能安全与教育法案》，拟要求大型前沿人工智能模型开发者建立安全保障、报告、披露等要求；加州 9 月通过包括《前沿人工智能透明度法》等立法，旨在推动以透明度为核心的人工智能监管，包括要求前沿模型开发者公开分享安全框架，详细说明评估、缓解和管理灾难性风险的举措。

整体看，美国人工智能立法面临新技术发展与治理、联邦权力与州权力、大企业与其他利益群体之间的复杂博弈。一方面，特朗普政府提出放松人工智能监管，包括 OpenAI、谷歌等科技公司认为碎片化监管会带来合规负担，应由联邦政府制定“最低标准”，确保全国范围内的一致性，避免企业陷入“州际法律冲突”。另一方面，反对限制州层面立法监管人工智能的阵营认为，目前联邦层面缺乏综合性人工智能规范，若禁止州立法，将导致人工智能监管“完全失控”，州立法并非“扼杀创新”，而是“划定安全边界”。

《大而美法案》中限制州人工智能立法条款的争议，反映出美国内部在关于人工智能监管方面就创新与权益保护之间如何平衡的理念冲突。最终，州权支持者获胜，后续州层面的立法也进一步加快步伐，体现了公众对人工智能技术风险的警惕。未来，美国人工智能分散立法、逐步推进的模式或将持续。

与此同时，欧盟内部也在《人工智能法》是否需要延期实施方面产生类似的争议。支持法律延期实施的阵营认为，现有监管框架抑制

了本土人工智能研发；反对延期实施的阵营则担心延期将削弱欧盟在全球人工智能监管中的领导地位。经过数月博弈，欧盟委员会于 7 月明确拒绝全面推迟法律实施，但随后发布《通用人工智能行为准则》细化合规指引，提出简化中小企业合规流程。这场博弈不仅暴露了欧盟在技术主权与产业竞争力之间的深层矛盾，更揭示了全球人工智能治理的复杂性，需要在创新、安全、公平之间不断调适的动态平衡。

专栏 4 欧盟《人工智能法》的实施争议及分析

欧盟《人工智能法》于 2024 年 3 月通过立法程序，同年 8 月正式生效。该法采用基于风险的分类分级监管模式，并对关键条款的适用采取逐步生效的模式，为制定配套指南和企业合规留出时间。2025 年 2 月，禁止的人工智能系统规定开始实施，8 月，关于通用目的人工智能模型、治理、处罚等规则开始适用。《人工智能法》相关配套指南、行为准则、模板等相继发布，不断增强法规的落地性与可确定性。

然而，欧盟《人工智能法》实施仍面临诸多问题。一方面，近 50 家欧洲企业于 7 月公开呼吁欧盟暂停实施《人工智能法》，提出为期两年的法规暂停计划，为提供更加清晰和简化的规则留出空间。另一方面，《人工智能法》多项配套规则、标准等制定难以达成共识，延期出台成为“常态”，如原定于 5 月发布的《通用人工智能行为准则》在 7 月发布。相关企业认为，《人工智能法》增加企业合规成本，削弱欧洲的竞争力，并且与相关法律重叠条款较多，合规的不确定性增加。最终欧盟委员会坚持法律的确定性至关重要，拒绝推迟实施《人工智能法》。

欧盟《人工智能法》实施面临的问题和挑战受到全球其他司法辖区的关注，法律实施过程中面临的严峻考验为其他国家提供参考，对各国人工智能立法模式和进程产生一定影响。

5 月，日本国会批准《人工智能相关技术研发及应用促进法》，以高位阶原则性立法确立促进创新、推动人工智能技术应用的立法导向，提出国家应当采取必要的立法和财政措施促进人工智能技术研发

和利用。**在机制层面，**成立专门机构，提出内阁应设立人工智能战略本部，全面、系统地推进人工智能相关技术的研发和利用，并对人员设置及职责进行规定。**在法律责任方面，**该法未专门设置违法处罚条款，通过允许政府调查技术发展动向、对企业进行指导等方法应对人工智能滥用风险，同时，法律要求企业配合政府推进相关举措。

欧盟成员国中，爱尔兰、波兰、西班牙等已根据欧盟《人工智能法》要求，相继推动国内法立法，对人工智能监管的主管机关、违法处罚、沙盒监管等进行规定。其中，意大利成为欧盟第一个出台综合规范人工智能使用的法律的国家，于 9 月通过《人工智能规定及政府授权法案》。该法对非法传播人工智能生成或操纵的内容、利用该技术实施欺诈和身份盗窃等犯罪行为规定了处罚措施，并在医疗、教育、司法、劳动等关键敏感领域设置了人工智能使用的具体规则。除了发达经济体，发展中国家也在积极推进人工智能综合立法。5 月，以防范风险和激励创新为双重目标的巴西人工智能法案提交巴西众议院，法案强调对公民基本权利的保护，一定程度借鉴欧盟风险分级监管思路，将人工智能系统分为“过度风险”“高风险”和“其他”三类并明确人工智能开发和使用的 17 项基本原则，旨在促进负责任的创新，确保人工智能系统安全可信，推动社会、经济和科学技术发展。

表 2　2025 年全球人工智能立法主要进展

地区	法规名称	主要特点	立法进程
欧盟	欧洲议会和欧盟理事会规定人工智能的统一规则，并修正	基于风险的立法模式。	已生效。关于禁止性人工智能实践、通用人工智能模

	300/2008 号等指令的 2024/1689 号条例		型等规则已开始适用。
日本	《人工智能相关技术研发及应用促进法》	侧重国家推动人工智能研发应用。	已生效。
韩国	《人工智能发展与建立信任基本法》	兼顾治理与发展。	已通过，2026 年生效。
意大利	《人工智能规定及政府授权法案》	涵盖医疗保健、司法、公共管理等场景使用人工智能的具体规则。	已通过，2025 年 10 月 10 日生效。
爱尔兰	《人工智能监管法案》	指定执行欧盟《人工智能法》的国家主管机构，规定违规行为处罚。	制定中。
波兰	《人工智能系统法案》	指定执行欧盟《人工智能法》的国家主管机构，设立支持创新章节。	制定中。
西班牙	《正确适用和治理人工智能法案》	指定执行欧盟《人工智能法》的国家主管机构，提出监管协调机制。	制定中。
巴西	《人工智能法案》	基于风险的立法模式。	制定中。

2.多路径推动人工智能法治实施

细化规则提升法律法规的落地性。人工智能综合性立法覆盖范围广，既涵盖法律概念，也涉及具体实践，法律的理解和实施面临诸多挑战。以欧盟为代表的经济体通过制定法律指南、规范指引、合规模板等，利用具体案例和细化要求为合规实践提供判定标准，推进法律一致、有效和统一的适用。2 月，欧盟委员会批准《关于人工智能法确立的禁止人工智能实践的指南》，为“不可接受风险”类别的人工智

能系统认定提供参考。7 月，欧盟密集发布《通用目的人工智能行为准则》《通用目的人工智能模型提供者指南》《通用目的人工智能训练内容摘要模板》等各项配套指南，为通用人工智能模型提供者履行合规义务提供更清晰的指引。8 月，欧盟委员会和人工智能委员会认定《通用目的人工智能行为准则》充分涵盖了《人工智能法》第 53 条和 55 条规定的义务，准则的签署方可通过遵守该准则证明履行相关法律义务。目前，谷歌、亚马逊、微软、OpenAI、Anthropic 等企业已签署准则，但 Meta 以“法律不确定性”为由拒绝，认为部分要求超出《人工智能法》范畴。9 月，韩国科学信息通信部发布《人工智能发展与建立信任基本法》执行条例草案，明确适用于生成式人工智能和高影响人工智能经营者的透明度义务、确定高影响人工智能的标准等。同时，韩国科学信息通信部宣布将在法律初始执行阶段引入行政处罚宽限期，实际上将形成延迟监管的状态。

创新人工智能监管与合规工具箱。人工智能法律规则的合规方式至关重要，它不仅关乎企业能否安全高效地开展创新，也关系到整个社会能否在秩序中享受技术红利。面对复杂且快速演变的人工智能技术，传统的监管和合规手段往往成本高昂且响应迟缓，因此迫切需要引入创新工具为安全的科技创新提供支持。相关国家探索通过提供实时指引、人工智能法服务台以及监管沙盒等工具，为创新应用提供“安全试错”空间，形成“事前引导—事中监测—事后优化”的监管模式。4 月，欧盟发布《人工智能大陆行动计划》，提出建立“人工智能法服务台”，为利益相关者，特别是小型人工智能解决方案提供商和部署

者提供关于《人工智能法》的量身定制的信息和指导，帮助他们理解和遵守法规。服务台通过提供模板、指南、网络研讨会和培训课程来简化程序，促进企业合规，减少合规成本。目前，奥地利和德国已经推出了国家人工智能服务台，欧盟委员会已经推出了《人工智能法》服务台和单一信息平台。4 月，英国金融监管机构推出“人工智能实时测试”项目，按照以原则为基础、以结果为中心的监管方法，协助参与测试的企业在金融服务方面开展创新的同时，完善灵活的监管方式。7 月，特朗普政府《人工智能行动计划》将建立监管沙盒作为推动人工智能应用的政策行动之一。新加坡 AI Verify 基金会和新加坡通信媒体发展管理局推出“人工智能保证沙盒”，为人工智能应用程序提供测试，对幻觉、不良内容、数据披露等风险进行 3 个月测试并为参与者提供案例报告。

3.人工智能责任归属法律问题持续受到关注

人工智能技术的自主性、黑箱性，责任主体的多元性等特征引发的侵权法律问题已不容忽视，人工智能侵权责任的认定和承担作为事后救济，发挥重要引导作用，2025 年各国对相关法律问题持续关注，并探寻相应的解决方案。

著作权侵权问题争议持续聚焦创新保护。当前，全球正积极探索人工智能训练数据和生成内容的知识产权保护边界。美国通过行政指引、地方立法与司法判例不断界定合理使用范围，欧盟则依托《人工智能法》及行为准则强化版权合规要求。各国均在技术创新与权利保护之间寻求平衡，呈现出多元化的监管与司法实践路径。美国联邦层

面尚未就生成式人工智能版权问题出台相关立法，但州层面已积极推进。4 月，阿肯色州通过《关于生成式人工智能工具生成的训练模型和内容所有权法》，在输出内容权属方面作出规定，明确内容提供者应享有生成式人工智能工具所生成数字内容的版权，但前提是该生成内容不侵犯现有版权。使用版权数据训练大模型的合法性问题持续成为美产业界关注的焦点，是否属于“合理使用”成为判断的关键。5 月，美国版权局发布《版权和人工智能：生成式人工智能训练》（预发布版本）报告，围绕使用受版权保护的作品训练人工智能模型是否属于合理使用进行分析。报告提出实践中存在两个情况，**一是**出于非商业目的使用，且不在输出中复制作品，该情况一般属于合理适用。**二是**在能够获得许可的情况下仍从盗版来源复制作品，并生成不受限制的内容，该情况不太可能符合合理使用的条件。然而，实践中许多情况介于两者之间。此外，司法实践也对相关问题进行引导。6 月，美国北加州地方法院对使用版权作品训练生成式人工智能作出两份判决，科技公司均以“合理使用”作为抗辩，并因属于“转换性使用”获得法院的有利判决。从美国的实践来看，在对“合理使用”的四项要素判断中，法院基本认可开发生成式人工智能属于“转换性使用”，但法院在关于盗版作品的使用、市场稀释等问题上存在较多分歧，强调需要基于案件的特定事实作出裁判。

欧洲在使用版权数据训练人工智能引发的侵权问题方面尚未形成规则性共识。欧盟《单一数字市场版权指令》规定在权利人未明确表示权利保留的情况下，出于文本与数据挖掘目的的复制和摘录可构

成合理使用。欧盟发布的《通用人工智能行为准则》补充细化《人工智能法》对版权保护的要求，在透明度和版权章节均涉版权合规要求，包括公布训练数据来源、采取技术保障措施防止模型输出侵权内容等。然而欧盟现有成文法规则尚无法适应生成式人工智能发展带来的挑战，如：《单一数字市场版权指令》设立的文本与数据挖掘例外中关于“合法获取（lawful access）”“适当退出（appropriate opt-out）”等法律概念定义不统一、退出技术机制不完善，欧盟成员国国内法实施存在差异。此外，《人工智能法》的版权规则属于程序性要求，不涉及版权侵权规则、版权侵权执法等实质性要求。在司法层面，使用受版权保护作品训练大模型受到法院关注。11 月，德国慕尼黑第一地区法院就德国音乐演出和作品复制权协会（GEMA）诉美国 OpenAI 公司著作权侵权案作出一审判决，认定 OpenAI 未经许可使用受著作权保护的音乐歌词训练 ChatGPT 模型的行为构成著作权侵权，判令其承担赔偿责任。

人工智能侵权责任综合性立法谨慎推进。人工智能系统的复杂性和产业链上主体的多元性给人工智能责任规制形成挑战，立法探索受到多重影响，进程较为缓慢。2 月，欧盟委员会发布 2025 年工作计划，明确撤回 2022 年发布的《人工智能责任指令》提案。5 月，欧洲议会内部市场和消费者保护委员会发布说明，指出撤回指令的三大原因：一是欧盟《产品责任指令》和《人工智能法》已经为人工智能侵权救济提供方案。二是《人工智能责任指令》的评估基于假设而非真实市场数据，缺乏可靠性。三是《人工智能责任指令》在程序法方

面的探索可能会造成不必要的复杂性，导致产生阻碍创新和增加合规负担的问题。

4.人工智能国际合作聚焦发展关切

区域和多边合作治理更加深化。多个国家通过共同签署联合声明、制定区域性指南等方式，在促进人工智能技术包容性发展、制定规范标准及推动跨国政策协调等方面加强协作，在全球和区域层面构建了更加系统化、规范化的人工智能治理体系。2 月，人工智能行动峰会在法国巴黎召开，中国、法国、印度、欧盟在内的超过 60 个签署方发布《关于发展包容、可持续的人工智能造福人类与地球的声明》，强调以“开放”“包容”和“道德”的方式开发和利用人工智能，呼吁加强人工智能治理的协调，倡导“全球对话”。《声明》提出促进人工智能的可访问性以减少数字鸿沟，确保人工智能开放、包容、透明、道德、安全、可靠和值得信赖，为人工智能创新发展创造条件，加强国际合作等六方面主要优先事项。2 月，东南亚国家联盟（ASEAN）更新《人工智能治理与伦理扩展指南》，系统梳理了生成式人工智能的独特风险，建议东盟制定区域适用的生成式人工智能测试基准和测试工具，鼓励开发者、部署者、云服务提供商及监管机构之间的协作，支持区域层面的人工智能负责任使用。

弥合智能鸿沟成为人工智能治理的重要议题。当前全球各国正积极推动人工智能发展应用，但受限于人才、数据、算力等发展不均，智能鸿沟不断加剧。2025 年，一些国家积极构建多边协同治理框架，保障发展中国家参与权，提升发展中国家技术与数字素养，确保各国

平等获取人工智能发展机遇。7 月，金砖国家发布《金砖国家领导人关于人工智能全球治理的声明》，提出关切南方国家需要，强调多边主义、合法性与数字主权，强调人工智能治理应切实注重个人数据保护，保障人类权益，确保安全、透明、可持续，且有利于弥合本国及国家间日益扩大的数字与数据鸿沟，把公平竞争与市场规范、数据治理、保护知识产权与维护公共利益的平衡等作为指导方针。8 月，联合国大会通过《人工智能独立国际科学小组和人工智能治理全球对话的职权范围和设立及运作方式》决议，决定设立“人工智能独立国际科学小组”和“人工智能治理全球对话”机制，开展政策讨论以加强全球人工智能治理，支持可持续发展目标并弥合数字鸿沟，借助现有的联合国和多利益攸关方机制，支持在发展中国家进行人工智能能力建设，弥合人工智能鸿沟，便利使用人工智能应用程序，并建立高性能计算方面的能力和相关技能等。

（二）数据治理法律制度不断完善，精细化治理纵深推进

1.细化人工智能数据治理规则并推动治理协作

相关国家通过政策协调与联合承诺，发布最佳实践指南，利用技术实施、风险管理和加强监管机构的互动等方式推动管理规则的一致性。2 月，澳大利亚、韩国、爱尔兰、法国和英国的数据保护机构签署《关于构建可信数据治理框架以鼓励开发创新和隐私保护型人工智能的联合声明》，旨在帮助人工智能生态系统参与者遵守数据保护规则并促进创新。《声明》中承诺，促进对人工智能训练背景下处理个

人数据的合法依据的共同理解，加强监管机构之间的互动，以强化人工智能系统、工具和应用程序的不同监管框架之间的一致性。5 月，美国国家安全局（NSA）联合网络安全与基础设施安全局（CISA）、联邦调查局（FBI）以及英国、澳大利亚、新西兰等国的网络安全机构，共同发布了《AI 数据安全：保护用于训练和运行 AI 系统的数据的最佳实践指南》，明确了三大核心目标：一是提高对人工智能系统在开发、测试以及部署全生命周期数据安全风险的意识；二是为每个阶段提供实用的人工智能数据保护最佳实践，并深入分析关键风险领域；三是鼓励采用强有力的数据保护措施，主动实施风险缓解策略，为人工智能系统构建安全且具韧性的基础。

主要经济体完善人工智能数据利用规则，构建覆盖全周期的风险评估与影响评价制度，通过强化数据最小化、透明度和问责制等原则和制度，在促进人工智能创新的同时，坚实守护个人的数据权利与数据安全。人工智能数据治理规则不再停留于原则性声明，而是向深度精细化和场景化发展，顺应人工智能技术迭代迅速的特征，强调治理框架的动态调整。2 月，法国数据保护机构（CNIL）发布了两项建议，旨在使人工智能实践遵守《通用数据保护条例》（GDPR）的相关要求，要求平台要告知个人并促进其行使权利，明确数据最小化、保留期限和数据库再利用等规则。4 月，美国国家标准与技术研究院（NIST）就更新的隐私框架《NIST 隐私框架 1.1 初次公开草案》公开征求意见，增加了关于人工智能和隐私风险管理的新内容，涉及人工智能数据训练、隐私攻击和偏见等方面。5 月，以色列隐私保护局发布了《隐

私保护法在人工智能系统中的适用》指南草案，面向公众征求意见，强调隐私法适用于人工智能开发和部署的所有阶段，规定了披露义务、问责机制、数据安全要求、数据主体权利、挖掘在线个人数据的限制等制度。芬兰数据保护监察员办公室发布了《人工智能系统开发和使用中的数据保护》指南，阐明了各组织如何确保个人数据在人工智能系统中得到合法使用，规定各组织机构必须评估数据保护风险、确定安全措施、选择处理数据的法律依据、遵守 GDPR 原则等。7 月，法国数据保护机构（CNIL）制定了《网络抓取数据应采取措施的相关指南》。该指南规定了包括数据最小化、排除敏感或私人数据、遵守反抓取信号以及透明度在内的保障措施。8 月，韩国个人信息保护委员会发布《生成式人工智能开发与应用个人数据处理指南》，将生成式人工智能分为开发、应用等四个阶段，提出各阶段安全措施与法律标准，构建以个人信息保护负责人为核心的治理体系，并会依据技术发展动态更新。9 月，韩国个人信息保护委员会通过《个人信息保护法》修正案，要求公共机构在引入和使用人工智能时，应建立个人信息影响评估标准。欧洲委员会发布大型语言模型系统隐私和数据保护指南草案，重点关注数据最小化和用户权利。

2.推动数据共享利用规则

推进公共机构数据共享和利用法律制度的构建。部分国家和地区通过立法明确公共数据共享和利用的范围，安全保障措施和监督机制等制度。2 月，马来西亚公布《数据共享法案》，规范了公共部门机构之间数据共享的条件和保护措施，旨在提高政策效率、保护健康和

安全、应对紧急情况以及服务公共利益。6 月，英国通过《数据（使用和访问）法》促进公共机构持有数据的利用。一是明确公共机构“以公共利益为导向”的具体数据共享场景；二是引入“公认合法利益”作为数据处理的法律依据，包括国家安全、公共安全与国防等；三是要求建立“数字验证服务信任框架”，允许公共机构向注册的验证服务提供商披露数据，以支持身份验证和服务交付。6 月，卢旺达出台国家数据共享政策，为政府数据共享作出规划，重点包括建立数据治理部门、技术小组委员会，制定数据标准提升互操作性，建立政府数据共享平台等，未来将要求政府部门使用数据共享平台进行所有政府间的数据共享。

企业间数据共享和利用规则进一步落实深化。以欧盟为代表的立法通过强制性规范打破数据垄断，明确互操作性要求和反不公平条款保障数据访问权，并辅以细致的行业指南确保落地，促进数据在更广范围内有序流动与利用。6 月，英国通过《数据（使用和访问）法》促进企业数据流通。一是要求数据控制者在客户或者授权的第三方提出请求时，共享结构化、机器可读的客户数据；二是在部分情况下，要求数据处理者公开商业数据；三是对数据的准确性和完整性等作出规定。7 月，欧盟委员会根据《数字服务法》通过了一项授权法案，规定大型在线平台和搜索引擎必须向研究人员提供对公开数据的访问权限。9 月，欧盟《数据法》施行，规定了欧盟市场上的互联设备的设计应当允许数据共享；应让制造业等行业的企业用户能够访问有关工业设备性能的数据，从而为提高效率和优化运营创造机会；让消

费者轻松传输数据并在云服务商之间切换; 禁止可能阻碍数据共享的不公平合同等。同月，欧盟发布《与法规 2023/2854（数据法案）相配套的车辆数据指南》，明确了《数据法》中定义的原始数据、预处理数据、推断或衍生数据，在汽车产品中的示例等内容。

完善数据跨境流动规则。部分国家和地区围绕跨境数据流动的合法依据、安全保障、风险评估、问责制等方面进一步细化规则，推进使用经过认证的标准化工具来简化合规流程，在数据主权与流动自由之间构建“风险可控的开放”。1 月，土耳其个人数据保护局发布了《个人数据向国外传输的指南》，明确了根据修订后的《个人数据保护法》第 9 条将个人数据传输到国外的流程。4 月，马来西亚个人数据保护部发布了《跨境数据传输指南》，详细说明了数据控制者的条件和义务，包括需要有效的法律依据、安全的传输方法以及维护数据接收者的记录。该指南建议进行传输影响评估，以确保接收国拥有同等的数据保护法，并强调使用标准合同条款和具有约束力的公司规则来实现合规性。6 月，欧洲数据保护委员会（EDPB）发布《关于向第三国传输数据的 GDPR 第 48 条指南》，明确欧盟实体应对第三国公共当局数据请求的合规框架，强调任何响应第三国当局的数据传输，均需符合 GDPR“两步测试”，既要满足第 6 条（数据处理的法律依据），也要符合第 5 条（跨境数据传输条件），确保不降低欧盟境内个人数据保护水平。同月，全球跨境隐私规则（CBPR）论坛启动了全球 CBPR 和处理者隐私识别系统，以促进参与经济体之间的可信数据流通。截至 9 月，共计 107 个参加组织，其中主要包括美国、日本、新加坡等

国家的企业。9 月，德国联邦与州独立数据保护监管机构会议发布《针对医疗科研领域国际数据传输的应用指南》，明确“两步审查”的合规方式，第一步审查数据处理法律基础、第二步审查向第三国传输的合法性基础，以解决在该场景下的适用《通用数据保护条例》的难点。

3.深化个人信息保护治理

推动个人信息保护规则精细化场景化。部分发达国家对个人信息保护规则不断进行深化和细化，从原则性规定走向场景化、精细化的可操作规则，深入规定如何获得真正合法、有效的同意，灵活调整数据留存期限。挪威新的《电子通信法》于 2025 年 1 月生效，要求 cookie 和类似技术的使用必须符合 GDPR 中告知同意的相关要求，并授予挪威数据保护机构（Datatilsynet）和挪威通信管理局（Nkom）相应的执法权力。法国数据保护机构（CNIL）发布了关于移动应用程序隐私保护的建议文件，明确不应将技术权限和用户同意混为一谈，规定同意必须是自由、具体、知情和明确的。4 月和 7 月，韩国个人信息保护委员会分别发布两个个人信息处理相关指南，细化个人“同意”具体情况，放开部分情况个人信息保留期限。8 月，韩国修订《个人信息保护法》，明确了个人信息可携权具体适用场景。

加强敏感个人信息保护。部分国家和地区进一步明确敏感信息的范围，实施数据处理全生命周期管控，强化处罚机制。4 月，马来西亚 2024 年《个人数据保护法（修正案）》有关敏感个人信息部分条款生效，纳入生物特征数据和数据泄露概念，要求数据处理者遵守安全规定，提高罚款额度等。同月，美国司法部制定的《关于防止受关

注国家或相关人员访问美国敏感个人数据和美国政府相关数据的规定》生效，禁止和限制与特定国家、人员进行数据交易，以防止有关国家获取和利用美国公民的大量敏感数据和政府相关数据。8 月，加拿大发布《联邦机构生物特征处理指南》，针对联邦机构处理生物特征信息的隐私义务提供指导，明确生物特征技术分生理型（如指纹、DNA）和行为型（如按键模式、步态），生物特征信息属于个人信息且多具敏感性，从合法权限、隐私影响评估、必要性与比例性等方面提出相应要求。

此外，一些国家和地区聚焦用户同意与透明度、特殊数据与群体保护，针对大型科技平台和拥有大量用户数据的新兴业态开展严格执法。例如，9 月，法国数据保护机构监管机构（CNIL）对谷歌处以 3.25 亿欧元（约合 3.8 亿美元）罚款，主要针对违反 Cookie 规则的行为。同月，美国判决谷歌支付 4.25 亿美元的罚款，因其在一起集体诉讼中被指控在用户选择退出跟踪的情况下仍收集用户数据。

（三）网络安全制度不断健全，重点领域规则持续深化

为应对人工智能、量子等新技术带来的机遇与风险，主要国家和地区不断完善网络安全领域的法律规范和政策指导，细化医疗、金融等应用领域网络安全规则。

1.网络安全管理制度持续完善

网络安全综合管理立法进一步细化管理要求，拓展管理手段。伴随全球网络安全挑战的升级，对数字经济发展带来严重威胁，域外国家积极修订完善网络安全法律制度，细化网络安全管理规则，健全充

实管理手段、协同合作机制，立法模式从“被动防御”转向“主动防御”和“协同响应”双轨并行，注重强化网络安全技术治理手段，深化供应链安全管理。1 月，欧盟通过《网络安全法》修正案，规定安全托管服务定义、认证规则等，旨在将安全托管服务纳入欧盟网络安全认证框架，并将欧盟各国已有的安全托管服务认证纳入统一规范，鼓励可信网络安全服务产业的发展。4 月，欧盟委员会就进一步修订《网络安全法》征求意见，重点关注网络安全机构职责任务、网络安全认证框架及信息通信领域供应链安全挑战，并探索进一步简化网络安全报告义务，优化欧盟商业环境。2 月，《欧盟网络团结法》生效，旨在加强欧盟检测和应对大规模网络安全威胁和攻击的能力。法律建议建立欧洲网络安全警报系统，以改进对网络威胁的检测、分析和响应。该系统将由欧盟各地的国家和跨境安全运营中心组成，使用人工智能和数据分析等先进技术来检测威胁并与跨境当局共享威胁警告，同时构建网络应急机制改进对网络安全事件的准备和响应，建立网络安全事件审查机制。4 月，英国政府提出了《网络安全和弹性法案》，将重点加强对供应链和关键国家服务的网络安全保护，具体内容包括：将更多实体纳入网络安全监管范围，包括数据中心、托管服务提供商和关键供应商等；为基本服务运营商和相关数字服务提供商设定更严格的供应链责任；加强监管机构权力，丰富监管工具；改进重大网络事件报告的标准等。5 月，日本国会众议院通过《促进主动网络防御等保障网络安全发展法案》，授权相关机构主动干预措施，规定当发现对政府机关以及供电、铁道、金融等关键基础设施的网络攻击时，

警察或自卫队可侵入对方网络系统实施删除攻击程序等无害化处置措施；建立常态化监控体系，对关键基础设施开展常态化网络巡逻；明确企业和个人的配合监管义务。6 月，欧盟成员国通过了《欧盟委员会关于欧盟网络安全危机管理蓝图》的提案，主要内容包括：应对欧盟层面的网络安全事件危机准备，网络安全危机事件识别、应对与恢复，加强与北约等合作。7 月，沙特阿拉伯国家网络安全局提出适用于政府机构、关键基础设施运营者、100 名以上员工私营企业的国家网络安全风险管理框架，明确网络安全风险管理流程，包括使用认证工具进行漏洞扫描、开展测试等，同时明确合规时间表，统一规范政府机构与私营部门的网络安全责任。10 月，新加坡数字发展与信息部（MDDI）和法务部向议会提交的《网络安全（救济与问责）》（“OSRA”）法案进行一读。法案提出设立在线安全委员会（OSC）作为专门机构，负责管理法定报告机制，使受害者能够就特定的网络伤害寻求及时救济，同时引入法定侵权责任，为网络侵害受害者提供获得救济的明确法律依据。

细化关键基础设施网络安全管理制度。关键基础设施安全成为各国网络安全监管的焦点，其核心是将风险管理责任制度化、具体化，并强调对供应链和运营中断风险的管控。部分国家推动立法，明确系统化的风险管理程序要求，安全事件与运营中断报告制度以及明确关键基础设施的范围。3 月，澳大利亚发布《关键基础设施安全（电信安全和风险管理计划）规则 2025》细化网络安全相关立法规范。该规则根据《关键技术设施安全法 2018》授权制定，针对电信这一关

键基础设施领域，明确了相关管理制度。一方面，明确关键基础设施出现重大风险的情形包括实质性失去对关键基础设施关键组件的访问权限、关键基础设施资产的功能中断或严重减速且持续时间达到无法管理的程度等 9 类；另一方面，明确责任主体对关键基础设施风险管理的要求，包括识别关键人员、确认责任实体、判断供应链风险、识别物理和自然危害等。6 月，加拿大政府提出 C-8 法案，拟制定《关键网络系统保护法》并修订《电信法》以保障加拿大电信系统安全。拟议的《关键网络系统保护法》明确关键网络系统定义，提出加强金融、能源、电信、交通、核工业等领域网络安全监管，要求被指定为关键网络运营商的主体制定网络安全计划、报告网络安全事件、识别供应链网络安全风险等。

2.新技术新业务网络安全风险管理制度持续健全

关注人工智能领域的网络安全挑战。一些国家主要通过“自愿性守则”与“强制性行政令”双轨并行的政策性制度，与推动人工智能安全技术研发等技术性措施相结合的方式应对风险。1 月，英国科学、创新和技术部发布《人工智能网络安全实践守则》及其实施指南，重点关注人工智能系统的网络安全风险应对。该自愿性守则提出人工智能全生命周期的网络安全管理应覆盖安全设计、安全开发、安全部署、安全维护和生命周期结束 5 个阶段，并提出各个阶段共 13 项人工智能系统的网络安全原则。6 月，特朗普签署《继续采取特定措施强化国家网络安全并修订 13694 号行政令和 14144 号行政令》，关注人工智能技术在网络安全领域的应用，提出人工智能有可能通过快速识别

漏洞、增加威胁检测技术的规模和自动化网络防御来提升网络防御能力，并要求通过数据开放和漏洞管理机制优化加强网络安全防御。具体包括：一是要求商务部、能源部、国土安全部和国家科学基金会在综合考虑商业机密与国家安全因素下最大限度向学术界开放现有网络防御研究数据集，加强网络安全研究；二是要求由国防部、国土安全部和国家情报总监协调白宫科技政策办公室、国家网络主任办公室及行政管理和预算局，将人工智能软件漏洞管理纳入现有漏洞管理流程及跨部门协调机制，加强网络安全防护协同。

关注应对量子计算带来的网络安全问题。量子计算破解当前主流公钥密码算法的能力持续提升，不断威胁数据保密性和系统完整性，各国以强制性行政指令或指导性路线图为驱动，以清晰的时间表为框架，采用基于风险的分级推进策略，动员和协调整个供应链和生态系统，共同向抗量子密码学时代迁移，并以此为契机提升整体的网络安全韧性和加密敏捷性。3 月，英国国家网络安全中心提出《迁移至后量子密码学的时间表》，提出通过迁移到量子计算机无法有效解决的密码学（后量子密码学）来缓解网络安全风险，并提出迁移的必要步骤，包括规划和评估需升级的设施和供应链，优先完成高风险系统的迁移，完成全系统适配等。6 月，特朗普《继续采取特定措施强化国家网络安全并修订 13694 号行政令和 14144 号行政令》明确量子计算威胁与应对方向，指出具有足够规模和复杂程度的量子计算能够破解美国和世界各地数字系统上使用的大部分公钥密码，要求美国国土安全部发布并定期更新支持后量子密码产品广泛可用的产品类别清单，

要求各机构尽快支持传输层安全协议 1.3 版或后续版本。6 月，欧盟发布《使用后量子密码学的协调实施路线图》，强调应将量子威胁作为相关实体风险管理的一部分，建立成熟的加密资产管理，以促进向后量子密码的过渡，并在总体上提高加密敏捷性。该路线图提出成员国应尽快推进向后量子密码学过渡，并最晚于 2026 年底初步制定成员国后量子密码过渡的路线图，采用基于风险的方法进行过渡时间安排，针对高风险和中风险启动过渡规划与试点，尽快对关键基础设施进行保护。

3.重点行业网络安全管理规范不断更新

各国进一步细化医疗、金融等行业领域网络安全规则，推动物联网等领域网络安全规范持续更新以适应新情况，对相关主体提出多维度量化管理要求。**医疗健康领域，**1 月，美国发布《健康保险流通与责任法》（HIPAA）关于受保护健康信息网络安全拟议规则，细化明确受监管实体的义务，包括要求相关医疗保健主体通过使用多重身份验证访问受保护健康数据、每六个月进行一次漏洞扫描、每年进行安全风险合规审计、在 72 小时内建立书面程序恢复受影响的系统和数据等提升网络安全能力。6 月，美国国会议员提出《2025 年医疗保健网络安全法案》，要求网络安全和基础设施安全局应与卫生与公共服务部加强协同，通过指定专员协调和联络卫生部门的网络安全问题、加强网络安全信息共享、开展医疗保健运营者的网络安全培训等加强联邦层面的部门协调，提升医疗保健和公共卫生部门的网络安全。**金融领域，**1 月，欧盟《数字运营韧性法》生效，对金融实体管理和应

对网络安全风险的信息通信技术风险管理框架、第三方风险管理、数字运营弹性测试、重大事件报告、网络威胁信息共享等进行规定，要求银行、保险公司、投资公司和其他金融实体拥有能够抵御、响应网络攻击或系统故障的能力，增强金融行业的数字运营韧性。**物联网领域，**5 月，美国国家标准与技术研究院发布《物联网产品制造商基础网络安全活动》初步草案，为物联网产品制造商提供网络安全实践建议，通过 7 项基础网络安全活动帮助制造商打造“可安全使用的物联网产品”，明确产品网络安全能力需覆盖物联网设备及后端、配套 APP、专用网关等组件。6 月，美国国家标准与技术研究院根据《2020 年网络安全改进法案》的要求，重新审视 2021 年发布的《联邦政府物联网设备网络安全指南：制定物联网设备网络安全要求》，推进物联网网络安全指南更新，从关注单一物联网设备的安全到全盘考虑整个物联网配套的产品安全，考虑如何将零信任架构、设备身份认证等技术融入物联网安全指南中。

4.完善促进基础设施建设法律规范

部分发达国家通过完善法律制度，简化行政审批、提出争议解决机制等推动信息通信基础设施共享，为推进基础设施部署提供保障。6 月，欧盟委员会启动针对《千兆基础设施法》第 3 条实施情况的专题咨询。该条重点规范现有电信基础设施的接入权等内容，欧盟委员会提出就基础设施接入的公平合理条款、运营商商业模式特征及争议解决程序等提供指导，以促进各方达成基础设施接入协议。7 月，德国联邦数字和国家现代化部发布修改和完善《电信法》的法律要点并

征求意见，强调通过完善法律法规支持德国光纤和移动网建设，包括完善相关实施细则，制定建筑物内光纤技术标准、优化建筑物内网络建设与共享规则、简化审批程序等。8 月，美国联邦通信委员会发布一项拟议规则，旨在简化电信基础设施环境审查流程、鼓励部署基础设施，从而推动电信行业的竞争和技术创新。主要拟修改内容包括明确监管范围、简化环境审查程序、完善协作机制与特殊规则，减少重复审查等。

（四）平台治理规则不断加强，主体责任规范不断完善

1.强化平台企业内容管理要求

加强人工智能生成内容管理。域外国家围绕内容标识要求，色情与隐私侵害以及政治领域等场景限制，针对人工智能生成内容进行规范，强化平台责任、加强受害者救济。4 月，美国通过《应对网页及网站中深度伪造引发的性剥削工具法》，明确将人工智能生成的信息内容纳入监管范围，旨在打击未经当事人同意传播裸照、私密视频等隐私内容，以及通过深度伪造技术合成色情内容的行为。该法还要求网络平台建立非法内容的快速删除机制，授权美国联邦贸易委员会（FTC）负责监督平台。8 月欧盟《人工智能法》通用目的人工智能模型相关义务生效，要求大语言模型生成的内容必须以机器可读的格式进行标注。

强化大型平台内容审查主体责任。一些国家通过司法判决、行政执法、配套规则等手段，强化网络平台对内容的管理责任，从强调“避风港原则”逐步转向“主动看门人”责任。6 月，巴西最高法院经过庭审

判定，部分推翻了《互联网公民权利框架》中的“避风港”原则（即平台通常不对用户发布的内容负责），要求平台对非法出版物的责任自用户通知之时开始，而非自其未遵守法院删除内容命令之时开始。对于广告或付费推广，平台的责任将被推定，即无论是否收到通知或法院命令，公司都将自动对其收到的、用于传播的出版物承担责任。在这些情况下，公司只有在证明其“已在合理时间内谨慎行事”删除了被视为违规的内容时，才可豁免责任。9 月，法国通过两项法令落实《确保和规范数字空间法》所规定的义务，一是要求每月来自法国领土的独立访客达 1000 万的在线平台保留被举报和删除的非法内容；二是要求制作色情音视频作品的生产商以及提供此类内容的在线平台对违法内容予以警示。英国宣布修订《网络安全法》，将自残内容升级为“优先违法行为”，强制要求社交媒体平台采取主动措施阻止内容发布，而非仅事后响应删除，要求平台通过技术手段预先识别并拦截自残相关内容，旨在减少其对用户的潜在伤害。

2.加强平台对特殊群体的保护责任

完善未成年人网络保护法规与相关规则。部分国家和地区针对儿童在线内容保护出台了针对性法规与规则，强化年龄验证要求，加强人工智能应用的未成年人网络保护要求，强调设置高级别的隐私和安全配置，规定举报与数据留存等风险响应机制，设置覆盖产品设计、运营的全链条保护制度体系。5 月，欧盟委员会就《数字服务法》下的未成年人网络保护指南草案启动公众咨询，拟规定验证用户年龄、改进向用户推荐内容的方式、默认将儿童账户设置为私密账户、儿童

安全内容审核的最佳实践、儿童友好的举报渠道和用户支持等内容。9 月，巴西出台《儿童和青少年数字法规》，全面强化平台责任，规定了平台应当从设计层面嵌入风险预防机制，实施可靠的年龄验证流程，提供家庭监督工具，快速处理非法、有害内容投诉与举报，规范未成年人个人数据处理等。10 月，美国加州出台法案（SB 243），要求人工智能陪伴型聊天机器人不得涉及自杀、自残或色情话题，必须每三小时提醒未成年人“正在与 AI 对话”，并建议其休息；开发人员还需要创建系统，防止他们的聊天机器人在与未成年人的对话中产生露骨的色情内容。

细化未成年人真实年龄验证规则。多个国家围绕未成年人年龄验证制定法律规则、实施指南等，通过强调数据最小化原则、明确验证技术要求、强制年龄阈值等机制，细化年龄验证管理要求。2 月，欧洲数据保护委员会（EDPB）发布了一份关于个人数据保护问题的年龄保证方法的声明，旨在引导企业遵守《视听媒体服务指令》《通用数据保护条例》和《数字服务法》关于年龄验证和儿童数据保护等相关要求，规定了确保年龄验证措施有效的评估原则。强调建立年龄保证机制的决定必须基于儿童存在实际风险，遵循法律规定的目的限制和数据最小化原则，要确保年龄核查措施的有效性和年龄验证处理的安全性。5 月，新西兰国家党议员向国会提交《社交媒体（有年龄限制的用户）法案》，要求社交媒体平台提供商采取合理措施，防止 16 岁以下的用户访问他们的服务。9 月，澳大利亚电子安全专员批准了六项行业制定的新行为准则，旨在加强对儿童的保护，防范包括人

工智能伴侣聊天机器人在内的有害内容风险，规定了色情网站等高风险内容平台必须采用适当的年龄验证技术，防止未成年人接触不良内容等。与此同时，澳大利亚电子安全专员为落实《2024 年在线安全修正案（社交媒体最低年龄）法》，出台了《社交媒体最低年龄监管指南》，要求社交媒体通过必要且相称的年龄验证方式处理个人信息。例如，采取合适的年龄验证系统、开发账号排查功能等措施，防止澳大利亚 16 岁以下青少年创建账号或保留已创建的账号。

3.完善网络消费者权益保护制度

部分国家通过修订或制定专项法律、准则及监管要求，从服务、营销等多维度强化网络消费者权益保护，监管制度从事后救济进一步迈向全过程保护，强化用户自主选择、不受骚扰等权益的保护。5 月，澳大利亚《电信消费者保护准则》修订，增加包括：提供负责任的销售、保护弱势消费者、增加电信服务质量保障、确保消费者在支付电信服务方面有多样化的选择、提供通俗易懂的信息以及数字可访问性要求等。同月，法国议会通过《关于加强电话营销管理及消费者保护以防止滥用法》，禁止任何人以营销为目的，向未表示同意的任何人拨打陌生电话；明确“客户例外”情形，与用户签订合同的公司可以打电话，但要求相关内容与所销售服务有关；大幅增加对电话营销有关的处罚，由三年监禁和 37.5 万欧元罚款提升至五年监禁和 50 万欧元罚款，对公司的罚款增加至其平均年营业额的 20%。6 月，比利时电信监管机构（BIPT）发布《关于修订 2005 年 6 月 13 日法案以加强电信市场消费者保护和赋权的第 458 号法案的意见》，要求 BIPT 每年发布在国家层面进行的比较价格的研究情况，在 BIPT 网站上以清

晰、可访问和互动的格式发布有关现有消费者权益保护的必要信息，向众议院提交年度报告说明其监督改善消费者保护条款的实施情况。7 月，墨西哥《联邦电信和广播法》在墨西哥联邦官方公报上公布，除引入机构重组外细化了对电信用户权益的保护，具体包括：明确由电信监管委员会负责用户权益保护，纳入不歧视和保护基本权利的原则；要求移动设备解锁交付，无论用户采用预付费还是后付费方案；明确对于未在原始合同中约定的附加服务，需事先获得客户同意后方可收费等。

4.规范网络平台竞争行为

构建适应本土市场环境的竞争管理规则。全球网络平台竞争管理规则延续“守门人”监管逻辑，同时部分国家结合本土市场痛点构建符合各国管理需求的法律规则。相关制度从打破生态封锁、禁止自我优待等反竞争行为、保障数据可携带与透明度、设立专门机构与严厉罚则等方面着手，管理重点从事后向事前延伸，增强用户和商家的自主选择权。5 月，美国议员提出《应用商店自由法案》，要求应用商店的运营者允许用户安装第三方应用商店或者选择第三方应用，开放开发者工具访问权限，并禁止应用内支付垄断，违规者最高面临单次 100 万美元罚款。7 月，日本公平贸易委员会和经济产业省通过了《智能手机特定软件竞争促进法》的实施条例和指南修正案，规定了智能手机操作系统提供商和应用商店确保公平竞争的具体义务，包括要求提供替代的应用程序分发和支付处理方案。9 月，巴西联邦政府向国民议会提交了一项法案，该法案修订了第 12,529/2011 号法律《巴西

竞争法》，通过具体制度设计减少数字生态系统市场准入壁垒，保护竞争过程，促进用户选择权。该法案规定了判断数字市场具有系统相关性的经济主体的认定标准，明确具有系统相关性经济主体的义务与禁止行为，包括应当进行信息透明度披露、用户权益保障，并在集中交易前提交监管部门审查，禁止自我优待、阻碍企业用户与终端用户直接对接等。9 月，泰国贸易竞争委员会针对《贸易竞争委员会关于不公平贸易行为及垄断、限制或减少数字服务（电子商务）多边平台竞争行为的指导方针（草案）》征求公众意见。草案旨在对电商平台展开严格监管，以遏制大资本挤压小商家、收取高额佣金、垄断物流以及跨应用窃取数据的行为，力求恢复小商家的公平竞争权利。

深入推进反竞争行为执法。部分国家和地区针对系统互操作性封锁、禁止转介与高额收费、自我优待、歧视性定价、附加不合理条件、广告市场支配地位滥用等问题开展执法。从措施上来看，呈现“事前监管+高额罚款+结构性救济”三重强化趋势。3 月，印度上诉法庭维持了印度竞争执法机构针对谷歌应用商店计费系统的处罚决定，即谷歌的应用商店收费政策对开发者而言是不公平且具有限制性的，但削减了罚款金额至 22 亿卢比。4 月，欧盟委员会对苹果公司处以 5 亿欧元罚款，主要针对苹果公司在其应用商店中限制应用开发者引导用户使用第三方渠道，剥夺了用户获取替代优惠服务的权利的行为。同月，日本竞争执法机构向谷歌公司发出禁止令，原因是谷歌公司以允许安装其应用程序商店为条件，要求部分手机制造商在所生产的手机上预装谷歌搜索和浏览器等软件，且软件图标须位于手机屏幕显眼位

置等。9 月，欧盟委员会以谷歌在在线广告技术领域滥用市场支配地位、在广告交易中偏袒自身服务为由，对其处以 29.5 亿欧元罚款，并得出初步结论，谷歌通过整改无法满足相关法律法规要求，可能需要剥离部分业务才能解决公平竞争问题。

表 3 部分国家和地区针对网络平台竞争行为的执法行动

行为类型	相关公司	典型表现	国家
保证互操作性	苹果	iOS 系统与第三方设备（例如智能手表或虚拟现实头戴设备）互操作性不足	欧盟
自我优待	谷歌、苹果	在搜索结果中优先显示其自营服务（如购物、酒店预订等）	欧盟
强制交易	苹果	限制应用开发者引导用户使用第三方渠道	欧盟
捆绑	谷歌	以允许安装其应用程序商店为条件，要求预装其他软件	日本
技术歧视	谷歌	滥用主导地位，扭曲在线广告市场竞争的行为	欧盟

四、2026 年互联网法治展望

历经多年探索与实践，我国互联网法治已取得显著进展，但新技术、新应用、新场景不断涌现，尤其是以人工智能为代表的科技飞速发展，已经成为推动社会进步和经济发展的重要力量。与此同时，科技的发展也导致网络空间的复杂性与日俱增，互联网法治建设面临全新机遇与挑战。党的二十届四中全会明确了“十五五”时期经济社会发展的主题主线，2026 年作为“十五五”的开局之年，互联网法治建设需要围绕党中央确定的目标任务，着眼加快建设网络强国、深入推进数

字中国建设，抓住人工智能等技术创新、数据要素价值释放等网络领域发展的关键性、决定性因素，把握好立法的节奏和进度，为网络强国和数字中国建设的稳步推进保驾护航。一方面不断巩固并拓展个人信息保护、数据跨境流动等领域的现有优势成果，另一方面聚焦数据和平台治理关键瓶颈问题全力突破，推动网络领域实现质量与效益的双重跃升。

（一）稳步推进人工智能法律制度体系建设

习近平总书记在中共中央政治局第二十次集体学习时指出：“要把握人工智能发展趋势和规律，加紧制定完善相关法律法规、政策制度、应用规范、伦理准则，构建技术监测、风险预警、应急响应体系，确保人工智能安全、可靠、可控。”我国人工智能发展迅速，在诸多领域取得显著成果。“十五五”期间是人工智能落地的关键窗口期，需要以促进人工智能健康有序发展为重要目标，完善互联网法治，全方位赋能“人工智能 +”从“蓝图”变为“实景”。目前我国人工智能立法尚处于逐步完善阶段，然而人工智能技术发展迅速，不确定性高。发展好、运用好、治理好人工智能，推动我国人工智能朝着有益、安全、公平方向健康有序发展，已经成为互联网法治工作面临的重大时代课题。2025 年全国人大常委会和国务院将人工智能健康发展立法列入年度立法工作计划。国务院《关于深入实施“人工智能+”行动的意见》提出，要“强化政策法规保障”“推进人工智能健康发展相关立法工作”。

下一步，建议坚持以良法善治保障人工智能发展的立法思路，妥善处理促进与规范之间的关系，瞄准当前和未来一定时间内人工智能的发展阶段，稳步推进人工智能法律制度体系建设。**一方面，**做好已有法律的适用工作，推进人工智能健康发展。**另一方面，**以包容审慎、总分结合的思维，既注重研究高位阶人工智能立法，也注重研究推进制定修订人工智能相关数据、算法、算力的要素立法和生成合成、拟人化互动、自动驾驶、智能助手、基因编辑等场景立法，通过明确人工智能发展治理基础性规则、破除阻碍人工智能发展的制度障碍、划定人工智能安全底线，推动形成我国人工智能治理的“制度名片”。

（二）健全完善数据法治基础护航新发展格局

当前，数据作为数字时代的新型生产要素，不仅是推动经济高质量发展和新质生产力形成的核心支撑，更成为人工智能创新迭代的关键基石。尤其随着人工智能基础超级模型、具身智能的发展，对训练数据供应提出新要求，人工智能行业数据集建设面临内容密集性、领域相关性、数据多样性和形式规范性等核心质量问题。因此，要准确把握我国数据治理面临的新形势新任务，面向通用人工智能和行业深度赋能，加快相关法律制度建设，助力强化学习、世界模型等前沿技术和行业智能体获取新型高质量数据集。同时，也要关注人工智能对数据合规、隐私保护、安全利用提出的新挑战。在法治轨道上持续推进数据发展和安全治理工作，以高水平数据法治建设护航数字经济高质量发展。

下一步，可综合考虑发展和安全、国际和国内、当下和长远三个方面，分类讨论数据供给、交易流通、安全保障、收益分配等方面的制度构建问题，激活数据要素潜能，塑造经济增长动力。**短期内**，结合行业立法和要素立法已有经验，一方面，明确促进创新的规范原则，修改《个人信息保护法》等相关法规法律，增加数据供给合法性基础。同时，出台相关指引，引导人工智能新应用相关主体合规。另一方面，明确公共数据资源授权运营的法律属性，规范公共数据资源授权运营实施，推进高质量数据集建设。**中长期**，一方面，持续推进基础制度供给，健全完善数据治理、数据安全等制度，加快构建覆盖数据收集、存储、传输、使用全流程的监管制度框架，明确各主体权责边界，更好保障数字经济安全发展，为市场主体营造稳定、可预期的制度环境。另一方面，持续关注人工智能等新技术发展情况，研究人工智能等新兴技术对数据相关立法的影响，结合行业发展，在时机成熟时推动《著作权法》修订，明确人工智能生成内容的法律定性与权利归属，推动人工智能相关立法进程，实现发展与安全的动态平衡。

（三）体系化构建网络信息内容生态治理长效规则

当前，数字技术正以前所未有的深度与广度融入社会生产生活各领域，网络空间已成为亿万民众共同的精神家园与经济社会运行的关键场域。同时，网络空间的快速扩张也衍生出一系列新矛盾与新风险，一方面，虚假信息、网络暴力、算法滥用等问题持续侵蚀网络生态根基，另一方面人民群众对清朗网络环境的诉求愈发强烈，对优质信息供给、公平数字服务、安全网络体验的期待不断升级。习近平总书记在中共中央政治局第二十三次集体学习时强调：“要健全网络生态治

理长效机制，着力提升治理的前瞻性、精准性、系统性、协同性，持续营造风清气正的网络空间。”

下一步，互联网法治可锚定管网治网的实践成效与现实需求，以顶层设计为引领明确治理方向，修订完善互联网信息服务管理的顶层立法，健全完善互联网信息服务管理的体制机制，构建协同治理格局，打通治理链条，深化治理效能。着力规范网站平台责任，督促网站平台建立高质高效的内容审核与风险预警机制，健全平台规则和内部管理制度。完善分级分类的安全监管机制，明确网络内容风险等级，构建阶梯式处置机制，健全系统化、精细化治理框架。明确人工智能等新技术新应用的信息服务内容管理要求，划定规则“红线”，通过系统化治理构建全流程防护屏障。不断完善垂直细分领域法律法规，持续针对自媒体、MCN 机构管理等方面，出台专门的规章制度，提升依法治网针对性、有效性。

（四）织密建强网络安全法治规则体系

当前，网络已成为支撑金融、能源、交通等关键信息基础设施运行的“神经中枢”，更是维护国家主权、安全与发展利益的重要战略空间。与此同时，网络空间对抗性与复杂性持续升级，人工智能、量子计算、卫星互联网、低空经济等新技术新应用的快速迭代进一步拓展了安全威胁边界与传导链条，新应用场景下风险向空域管理、空间通信、公共安全等领域延伸，多重风险交织叠加，关键信息基础设施面临的安全威胁更趋多元复杂，对现有安全防护体系和制度带来严峻挑战。党的二十届三中全会就“推进国家安全体系和能力现代化”作出全

面系统部署，明确提出“加强网络安全体制建设，建立人工智能安全监管制度”，党的二十届四中全会提出“要健全国家安全体系，加强重点领域国家安全能力建设，提高公共安全治理水平，完善社会治理体系”。

下一步，互联网法治可立足“十五五”时期网络安全发展的新需求与新挑战，加快推进《网络安全法》《数据安全法》配套法规制度的修订完善，健全网络安全等级保护等核心制度。不断完善人工智能安全监管制度和标准规范体系，从人工智能全生命周期全要素明确规范要求，制定人工智能行业应用安全指南，为常态化开展人工智能安全风险监测提供制度依据。围绕量子信息、卫星互联网、低空经济等新技术新应用，加强前瞻性安全管理制度研究，确保新技术新应用安全健康有序发展。坚持“统筹全局”与“精准施策”相结合，不断细化关键信息基础设施认定、数据分类分级保护等配套制度，提升网络安全法治的针对性与可操作性。推动建立跨部门、跨区域的协同执法机制，加大针对网络攻击、网络诈骗、侵犯公民个人信息等违法犯罪行为的打击力度。完善行政执法与刑事司法衔接机制，提升网络空间执法效能。

（五）夯实涉外法治根基服务网络空间发展全局

随着全球数字化进程的加速，互联网领域的国际竞争与合作日益频繁，国际社会对数字经济规则制定的关注度不断提高，数据跨境流动、人工智能等新兴技术领域的规则博弈加剧，国际竞争越来越体现为制度、规则、法律之争，涉外法治建设对于维护国家主权、安全和

发展利益的重要性、紧迫性更加凸显。党的二十届三中全会提出“完善高水平对外开放体制机制”“稳步扩大制度型开放”；党的二十届四中全会提出要“扩大高水平对外开放，开创合作共赢新局面”。这对强化涉外法治的引领作用，完善公开透明的涉外法律体系提出了更高要求。

下一步，面向“十五五”，我国可在电信市场准入、跨境数据流动、个人信息保护等领域对接、积极吸纳高标准国际经贸规则，推进有关法律和行政法规制定修订，形成与国际通行规则相适应的法律框架，夯实高水平开放的法治根基。此外，我国可在人工智能、数据治理等方面积极参与国际规则制定，推动在联合国、世界贸易组织等多边体系框架下，形成公平合理的网络空间治理国际规则，提升我国国际影响力、感召力、塑造力。同时，可持续在数据跨境流动、新兴技术及电信服务等领域，探索加强双边规则谈判与务实合作，持续扩大与其他国家、地区的网络治理规则共识。继续推进与“一带一路”国家和地区的数字贸易协作，构建数字经济领域国际法律合作机制，着力提升我国在全球数字治理中的话语权，为全球数字经济可持续发展提供更多中国智慧。

附录：2025 年互联网领域立法梳理

效力位阶	名称	发文字号	发布日期	实施日期
法律	《中华人民共和国民营经济促进法》	中华人民共和国主席令第四十六号	2025.04.30	2025.05.20
	《中华人民共和国反不正当竞争法》	中华人民共和国主席令第五十号	2025.06.27	2025.10.15
	《中华人民共和国海商法》	中华人民共和国主席令第五十八号	2025.10.28	2026.05.01
	《全国人民代表大会常务委员会关于修改〈中华人民共和国网络安全法〉的决定》	中华人民共和国主席令第六十一号	2025.10.28	2026.01.01
行政法规	《公共安全视频图像信息系统管理条例》	中华人民共和国国务院令第 799 号	2025.01.13	2025.04.01
	《政务数据共享条例》	中华人民共和国国务院令第 809 号	2025.05.28	2025.08.01
	《互联网平台企业涉税信息报送规定》	中华人民共和国国务院令第 810 号	2025.06.20	2025.06.20
部门规章	《个人信息保护合规审计管理办法》	国家互联网信息办公室令第 18 号	2025.02.12	2025.05.01
	《人脸识别技术应用安全管理办法》	国家互联网信息办公室、中华人民共和国公安部令第 19 号	2025.03.13	2025.06.01
	《人工智能气象应用服务办法》	中国气象局、国家互联网信息办公室令第 45 号	2025.04.23	2025.06.01
	《中国人民银行业务领域数据安全管理办法》	中国人民银行令〔2025〕第 3 号	2025.05.01	2025.06.30
	《国家网络身份认证公共服务管理办法》	中华人民共和国公安部、国家互联网信息办公室、中华人民共和国民政部、中华人民共和国文化和旅游部、国家卫生健康委员会、国家广播电视总局令第 173 号	2025.05.19	2025.07.15
	《关键信息基础设施商用密码使用管理规定》	国家密码管理局、国家互联网信息办公室、中华人民共和国公安部令第 5 号	2025.06.11	2025.08.01
	《个人信息出境认证办法》	国家互联网信息办公室、国家市场监督管理总局令第 20 号	2025.10.14	2026.01.01

效力位阶	名称	发文字号	发布日期	实施日期
法律法规配套规范文件	《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》	发改数据〔2025〕18 号	2025.01.06	2025.01.06
	《公共数据资源登记管理暂行办法》	发改数据规〔2025〕26 号	2025.01.08	2025.03.01
	《公共数据资源授权运营实施规范（试行）》	发改数据规〔2025〕27 号	2025.01.08	2025.03.01
	《关于建立公共数据资源授权运营价格形成机制的通知》	发改价格〔2025〕65 号	2025.01.16	2025.03.01
	《互联网军事信息传播管理办法》	军政〔2025〕26 号	2025.01.22	2025.03.01
	《关于加强新时代审判工作的意见》		2025.02.08	2025.02.08
	《全国数据资源统计调查制度》	国数综资源〔2025〕26 号	2025.02.18	
	《卫星网络国内协调管理办法（暂行）》	工信部无〔2025〕52 号	2025.03.04	2025.05.01
	《人工智能生成合成内容标识办法》	国信办通字〔2025〕2 号	2025.03.07	2025.09.01
	《网络交易合规数据报送管理暂行办法》	国市监网监规〔2025〕2 号	2025.03.24	2025.04.25
	《促进和规范金融业数据跨境流动合规指南》		2025.04.17	
	《终端设备直连卫星服务管理规定》	国信办发文〔2025〕1 号	2025.04.23	2025.06.01
	《网信部门行政处罚裁量权基准适用规定》	国信办通字〔2025〕3 号	2025.06.26	2025.08.01
	《关于印发数据流通交易合同示范文本的通知》	国数综政策〔2025〕78 号	2025.07.02	2025.07.02
	《工业和信息化部行政执法事项清单（2025 年版）》	工信厅政法函〔2025〕300 号	2025.07.18	2025.07.18
	《网络交易平台收费行为合规指南》	国家市场监督管理总局公告 2025 年第 32 号	2025.07.31	2025.07.31
	《关于优化业务准入促进卫星通信产业发展的指导意见》	工信部信管〔2025〕180 号	2025.08.25	2025.08.25
	《宗教教职人员网络行为规范》	国宗发〔2025〕12 号	2025.09.07	2025.09.07
	《国家网络安全事件报		2025.09.11	2025.11.01

效力位阶	名称	发文字号	发布日期	实施日期
	告管理办法》			
	《关于治理价格无序竞争 维护良好市场价格秩序的公告》	中华人民共和国国家发展和改革委员会、国家市场监督管理总局公告 2025 年第 4 号	2025.09.28	2025.09.28
	《政务领域人工智能大模型部署应用指引》		2025.10.10	2025.10.10
	《能源行业数据安全管理办法（试行）》	国能发规划规〔2025〕108 号	2025.12.08	2026.07.01
	《互联网平台价格行为规则》	发改价格规〔2025〕1607 号	2025.12.09	2026.04.10
	《关于规范网络名人账号行为管理的通知》		2025.12.26	2025.12.26
征求意见稿	《网络信息内容多渠道分发服务机构相关业务活动管理规定（草案稿）》		2025.01.10	
	《直播电商监督管理办法（征求意见稿）》		2025.06.10	
	《可能影响未成年人身心健康的网络信息分类办法（征求意见稿）》		2025.06.13	
	《汽车数据出境安全指引（2025 版）（征求意见稿）》		2025.06.13	
	《中华人民共和国价格法修正草案（征求意见稿）》		2025.07.24	
	《直播电商落实食品安全主体责任监督管理规定（征求意见稿）》		2025.08.01	
	《人工智能科技伦理管理服务办法（试行）（公开征求意见稿）》		2025.08.22	
	《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》		2025.09.12	
	《促进和规范电子单证应用规定（征求意见稿）》		2025.09.13	
	《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》		2025.09.16	

效力位阶	名称	发文字号	发布日期	实施日期
	《互联网平台反垄断合规指引（征求意见稿）》		2025.11.15	
	《网络安全标识管理办法》（征求意见稿）		2025.11.21	
	《大型网络平台个人信息保护规定（征求意见稿）》		2025.11.22	
	《网络数据安全风险评估办法（征求意见稿）》		2025.12.06	
	《人工智能拟人化互动服务管理暂行办法（征求意见稿）》		2025.12.27	

中国信息通信研究院 互联网法律研究中心

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62302632

传真：010-62302476

网址：www.caict.ac.cn