公安部第三研究所
网络安全法律研究中心

360

西交苏州信息安全法学所

# 全球网络安全政策法律发展年度报告

# （2024）

公安部第三研究所网络安全法律研究中心

360 集团法务中心

西交苏州信息安全法学所

# 前　言

这是一个“大网络安全法”的时代。

作为长期跟踪全球网络安全政策法律演进态势的专业团队，我们亲历了网络安全政策法律如何从早期的边缘学科发展为如今的热点议题。可以观察到，几乎所有的现代立法均已或正在尝试对领域内的网络安全问题建章立制或预留制度接口，甚至网络安全政策立法的态度也成为判断特定问题走向的“晴雨表”。这得益于技术驱动社会信息化、网络化、数字化和智能化的客观发展，网络安全内涵的不断外扩与细分，早期单向度的“防御攻击”治理目标已经仅仅成为“大网络安全”观念的一部分。当前的网络安全规范系统变得更为复杂多变，任何既定规则的不确定性都会如蝴蝶效应那般产生几乎无法预见的规制后果，无论对个人、组织抑或国家。当然，这可能是“熵增”的必然结果，也使政策法律如何发挥“工具性价值”变得更为专业。

回顾网络安全法治历程，其始终是由技术驱动的。人类进入信息社会的经验和教训使得规范系统的构建在一开始就成为必须和技术应用同步考虑的问题，这在短时期内促成了国内外网络安全政策法律的高度繁荣。从没有哪个时代像今天这般高度依赖某一特定技术的底层支撑，这不仅是便利性问题，更是生存和发展的问题。如果追本溯源，那么“技术恐慌”无疑是不可忽视的重要内在驱动，信息时代的“技术奇点”频繁而影响深远，且技术本身开始愈发体现出不可见性或不可解释性，对于“未知的未知”，人类的安全观念始终试图实现可预期的控制，但这正在变得更为困难。时至今日，已经很难剥离技术本身而探讨社会治理问题，我们加速完成了由人机交互向人机融合的过渡转向，这一过程建立起虚拟与现实之间几乎可以触碰到的关联

性。这也是当前为何我们在某一风险成为普遍性社会威胁前，就开始尝试构建一种基于“泛安全化”的规范系统，因为风险本身可能已经远远超越我们的理解。在人工智能带来的影响尚在人类理解范围之内时，对这种影响加以考量，尝试以人类价值观和法律工具等进行塑造，正是对当下全球人工智能政策立法蓬勃发展状态和阶段的一种理解。

“大网络安全法”时代由此而来。

2024 年，网络安全政策法律的这一时代特点表现得更加明显，尽管我们仍然可以归纳出人工智能、数据、算法等热点关键词，但网络安全的议题范围几乎已经涵盖到社会运行的全部，网络安全呈现与地缘政治、新兴技术、价值供应等要素更为密切和主动的融合态势，各国发生的诸多网络安全方面的政策法律、事件、案例等都蕴含着上述因素的影响。全球网络安全政策法律仍然体现出明显的风险导向和特定判断的特点。在人类社会发展的任何历史时期，对于普遍性社会问题治理的思路始终是围绕风险或威胁展开。简单而言，网络安全的本质就是人类生产生活向信息和信息系统迁移过程中的生存和发展问题，面向越来越明显的技术“不可见性”，对于“未知”和“失序”的担忧无疑将变得更为强烈，这构成所谓多维度竞争关系的关键内核。

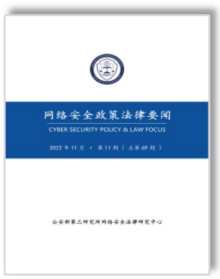
本报告第一部分通过归纳美国、欧盟、英国、法国、德国、俄罗斯、澳大利亚、加拿大、新西兰、新加坡、日本、韩国、巴西、中国等国家和地区在同一“行动域”的政策法律情况，直观展示全球立法特点和核心内容，总结 2024 年全球网络安全政策法律发展情况，宏观把握法治走向；第二部分基于历年特别是 2024 年全球网络与数据安全态势，对 2025 年乃至更长时期内的政策法律趋势进行研判。附件部分基于 2024 年政策与法律整体分析，分别遴选出境外和境内网络安全政策法律领域 2024 年十大事件。

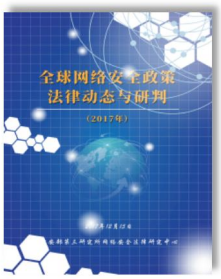
本报告将2024年全球网络安全政策法律发展总结为十大特点：（一）局部区域冲突延宕，竞争与合作交织并存；（二）关基安全保护规则持续细化，实践应用日益深化；（三）数据安全政策立法蓬勃发展，安全与发展导向深度调整；（四）个人信息保护立法不断完善，执法力度持续强化；（五）供应链安全政策立法持续发展，各环节规则日臻完善；（六）信息内容治理成为关注焦点，各国侧重有所不同；（七）人工智能不同法治形态蓬勃发展，推动发展与安全的辩证统一；（八）网络安全基石作用日益凸显，密码相关政策法律加速推进；（九）虚拟货币全球监管格局形成，涉加密货币犯罪打击成为热点；（十）网络犯罪链条打击共识初步形成，首部具备普遍法律约束力的全球性国际公约通过。

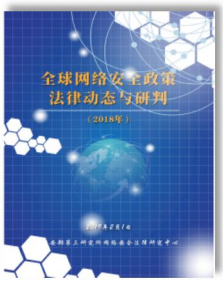
本报告认为，未来技术、颠覆性技术的不确定性日益增强，重大事件驱动重大立法的规律将被反复验证，云计算、大数据、抗量子密码、人工智能、虚拟货币等引发的社会变革及其融合治理趋势进一步凸显。从中国乃至全球视角展望2025年乃至更长时期内，网络空间政策法律或将呈现以下十大趋势：（一）合作与竞争持续同频共振，中国企业出海法律环境更为复杂；（二）关基安全融入新型风险，供应链安全成为治理关键；（三）数据利用规则补足完善，数据法治扩展至生态治理；（四）个人信息保护规则调整，回应人工智能技术发展需求；（五）供应链安全治理在不同领域扩张，规则不确定性仍然突出；（六）信息内容治理的政治性趋向加剧，关注人工智能非法应用打击；（七）人工智能法治综合发展，各环节协同演进；（八）密码法治持续完善，技术革新与政策响应同步加速；（九）虚拟货币发展迅猛，完善安全监管成为必然；（十）科学化与法治化交融，趋向生态治理和干预治理转型。

# 说 明

自 2017 年起，公安部第三研究所网络安全法律研究中心始终密切关注全球网络安全相关政策法律动态，持续跟踪全球政策法规、热点事件及典型执法案例，并每月编撰《网络安全政策法律要闻》。同时，研究中心连续七年与国内科研机构、知名院校和一流企业合作，在二十余位中国网络安全法律领域权威专家的指导下，联合发布《全球网络安全政策法律发展年度报告》。该报告坚持公开发布，旨在与产学研各界共议发展情况、共输洞察观点、共探研究方向、共商前沿对策，为贯彻落实“坚持高质量发展和高水平安全良性互动”贡献一份学术力量。








## 联合出品

公安部第三研究所网络安全法律研究中心

360 集团法务中心

西交苏州信息安全法学所

## 指导单位

密码法治实践创新基地

中国信息安全法律大会专家委员会

中国抗量子密码战略与政策法律工作组

## 参编单位

网络安全等级保护与安全保卫技术国家工程研究中心

信息网络安全公安部重点实验室

上海市信息网络安全管理协会互联网安全法律服务专家委员会

上海市法学会科创法治研究会

数字丝路安全智库

西交科教院网络安全法治研究所

江苏竹辉律师事务所

北京中企数安咨询有限公司

## 公安部第三研究所网络安全法律研究中心

公安部第三研究所网络安全法律研究中心隶属于公安部第三研究所。中心致力于服务网络安全工作需要，积极开展前瞻性、对策性、应用性研究，跟踪研判境内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用带来的网络管理热点难点问题，广泛开展学术交流研讨和产学研合作，为网络安全监管机构提供高质量的法律研究支撑，引领和推动我国网络安全法治发展。

邮箱：cslaw@gass.ac.cn　　公众号：公安三所网络安全法律研究中心

## 360 集团法务中心法律研究

360 法律研究是隶属于 360 集团法务中心的高端智库。旨在依托 360 集团卓越的网络安全技术、多元化的产品形态和丰富的法律实践，围绕数字经济发展的前沿性问题，立足国家安全和行业发展，通过开放合作的研究平台，汇集各界智慧，协同解决互联网行业新型法律问题，为共建网络空间命运共同体提供战略支撑，理论保障和人才支持。

邮箱：g-zq-law@360.cn　　公众号：360 法律研究

## 西交苏州信息安全法学所

西交苏州信息安全法学所是我国最早成立的、专门从事信息安全法学研究的科研机构，负责“密码法治实践创新基地”具体运行和建设，获批苏州市总体国家安全观教育参观点、苏州市网络安全教育实训基地等资质。法学所致力于为国家网络与信息安全法治建设提供软科学研究，推动国家信息安全法治建设以及高层次复合型网络与信息安全人才培养，为企业网络与数据安全合规提供咨询。

邮箱：xieyonghong2015@xjtu.edu.cn　公众号：苏州信息安全法学所

## 顾问专家组

马民虎 密码法治实践创新基地 主任

严　明 公安部第三研究所/第一研究所 原所长

宋燕妮 全国人大常委会法工委经济室 原副巡视员

金　波 公安部第三研究所 副所长

刘晓庆 360 集团 总法律顾问

张　薇 情报杂志 主编

陈欣新 中国社会科学院法学研究所 研究员

李新友 国家信息中心 研究员

陈晓桦 中国信息协会信息安全专业委员会 常务副主任

李世刚 复旦大学法学院 副院长

## 报告指导组

吴松洋 公安部第三研究所 研究员

杨　涛 公安部第三研究所 研究员

黄道丽 公安部第三研究所 研究员

鲍　亮 公安部第三研究所 副研究员

李　豪 360 集团法务中心 总监

丁　月 360 集团法务中心 资深法律顾问

原　浩 西交苏州信息安全法学所 资深研究员

朱莉欣 西交苏州信息安全法学所 执行所长

于月霞 宁夏公安厅十一处 总工程师

赵　鹏 中国电信集团市场部产品二处 处长

赵　艳 华为中国区 网络安全与隐私保护总监

孙艳玲 北京快手科技有限公司法务部 高级总监

顾　伟 淘天有限公司 法务数据合规负责人

易　晨 中国香港港专学院 协理副校长

李　晶 国网湖北省电力有限公司数字化部网络安全处 处长

侯　亮 国泰君安证券股份有限公司 首席信息安全专家

刘春梅 上海市信息网络安全管理协会 秘书长

## 核心编制组

何治乐 胡文华 梁思雨 杜　虹 胡柯洋 王京华 王彩玉

吴若恒 李　坤 马　宁 洪慧英 陈晓霖 谢永红 方　婷

# 目 录

1

# 一、 2024 年全球网络安全政策法律发展回顾

在早期的网络安全理解中，“防御对信息和信息系统的攻击、破坏活动”被视为规范系统的主要任务，这一点到今天为止仍然没有改变，只是应对过程变得更为棘手，各国在防御式的网络安全政策法律领域投入更多精力。鉴于网络安全已经成为全球性威胁，各国在网络安全领域的合作开始变得愈发紧密。此外，将网络安全“泛安全化”的进程同样是近年来政策法律研究普遍关心的议题，网络安全正在超越既有边界，开始被植入更多的竞争要义。2024 年，科技领域的较量升级至前所未有的白热化阶段，特别是在半导体、人工智能等颠覆性技术疆域，包括中美在内的国家竞争态势尤为激烈且充满张力。概括而言，全球网络安全政策法律依旧高度繁荣，“冲突与合作”仍然是主旋律。各国对于新兴网络安全议题的反应更加迅速，在重点领域取得诸多进展。

## （一）局部区域冲突延宕，竞争与合作交织并存

2024 年国际秩序重塑与利益格局调整仍处于深刻而复杂的蜕变期。全球网络空间中，一方面各国在经济、政治等多个安全层面和维度的角逐依然激烈，俄乌冲突延宕、巴以冲突扩大蔓延背景下的外溢风险加剧，网络空间“升格”为主要战场，为全球安全格局增添诸多不确定性，安全风险的应对机制面临严峻挑战；另一方面，全球主要经济体在既有的地缘政治经纬上加强合作，探索网络空间中的数字经济贸易、智能科技创新等方面的新型合作路径。

### 1. 局部区域冲突延宕，外溢影响持续扩散

自 2022 年开始的俄乌冲突、2023 年开始的巴以冲突仍在深刻影响着全球局势，战场冲突逐渐扩散至其他领域。2024 年，俄罗斯宣布调整对乌网络作战，从早期针对民用关键基础设施的攻击转向更侧重军事目标的战术性网络行动。俄罗斯还调整网络部队的定位，帮助定位乌克兰的军事装备和阵地，表明网络部队与常规部队之间的协同更加紧密。为应对俄罗斯网络威胁，欧盟、乌克兰、英国宣布采取应对措施。德国国防部成立网络和信息部队（CIR），负责应对俄罗斯对北约成员国日益增加的网络攻击，保护电子基础设施以及分析虚假信息和其他混合威胁。欧盟第三届网络对话活动中，欧盟与乌克兰达成加强网络安全合作的共识，同意在态势感知、网络风险评估、网络危机管理、网络制裁等方面进行信息交流。欧盟承诺继续支持乌克兰的网络防御，提高东部伙伴关系国家的网络复原力。乌克兰国防部宣布成立网络事件响应中心，旨在加强对乌克兰军事和通信网络的防护，实现对网络事件的全天候监控与响应；英国政府宣布对三家俄罗斯组织和三名个人参与克里姆林宫虚假宣传活动，破坏国际社会对乌克兰支持的行为实施制裁。

巴以冲突方面，以色列、巴勒斯坦背后的支持方在巴以热战以外开辟新战场。美国财政部外国资产控制办公室（OFAC）宣布对伊朗伊斯兰革命卫队网络电子司令部（IRGC-CEC）对美国医院的勒索软件攻击、对欧洲国家和以色列的恶意网络活动实施制裁；同时，对2家伊朗公司和4名伊朗公民对十几家美国公司和政府实体发起鱼叉式网络钓鱼、恶意软件攻击等形式的网络攻击以及窃取数十万企业员工账户的活动实施制裁。

美国网络安全和基础设施安全局（CISA）与联邦调查局（FBI）发布《如何防止伊朗针对与国家政治组织相关的账户》报告，应对伊朗利用电子邮件和聊天应用程序等使用社会工程策略，对美政治活动和官员进行的黑客攻击。FBI表示，已确认伊朗曾干预特朗普的竞选活动，并且试图通过社交手段接触两大党派的总统竞选活动。CISA和FBI警告美国公民注意新账户或电话号码的未经请求的联系，以及任何异常的电子邮件请求或尝试通过社交媒体传递链接或文件。两机构建议使用防网络钓鱼的多因素身份验证和密码管理器，并直接访问网站来验证可疑警报。可以认为，由于网络空间的技术特点，以及由此导致的国际（法）秩序失灵，俄乌冲突、巴以冲突的风险正在快速叠加、外溢，这些“非传统”战争的显著特征，为主要大国通过联合国或其他多边机制抑制战争的升级或全面爆发增加了极大困难。

## 2. 贸易竞争摩擦不断，企业出海面临挑战

2024年，科技领域的较量升级至前所未有的白热化阶段，特别是在半导体、人工智能等颠覆性技术疆域，竞争态势尤为激烈且充满张力。美国将中国、俄罗斯等国家视为对手国家，联合盟友通过采取出口管制、遏制打压科技企业等极具策略性的行动，加剧技术断层和产业链供应链断裂风险。

美国敦促荷兰阻止半导体设备制造商 ASML Holding NV 为中国客户在设备销售限制实施前购买的敏感芯片制造设备提供服务和维修; 要求韩国对向中国出口半导体技术采取类似美国已实施的出口管制; 要求日本公司限制向中国出口芯片制造所需的光刻胶等。美国政府宣布自 9 月 29 日起，全美范围内将正式禁止使用俄罗斯网络安全厂商卡巴斯基实验室的所有软件产品。美商务部部长雷蒙多表示，禁令旨在隔绝任何可能被外国对手利用的弱点，保护美国信息通讯技术和供应链安全。

在对科技企业的制裁方面，最受关注的莫过于美国及其盟友对 TikTok 的遏制打压。4 月，时任美国总统的拜登签署《保护美国人免受外国对手控制应用程序侵害法》，即《TikTok 剥离法》，要求字节跳动必须在 270 日内剥离旗下应用 TikTok 的美国业务，否则 TikTok 将在美国面临全国性禁令。5 月，TikTok 提起诉讼，主张该法违背美国宪法第一修正案“保护言论自由”精神，以及立法极具针对性，违背平等保护条款，应接受更严格的审查。受美国影响，TikTok 在加拿大也面临类似困境，11 月 6 日，加拿大创新、科学和工业部部长发表声明称，经过国家安全审查程序，加拿大政府决定关闭 TikTok Technology Canada, Inc.在加业务。美国最高法院在 2025 年 1 月 17 日作出正式判决，以 9:0 裁定该法合乎美国宪法，要求其母公司字节跳动在 2025 年 1 月 19 日前剥离其在美国的业务，否则将面临全面禁用。2025 年 1 月 20 日，美国总统特朗普宣誓就任美国第 47 任总统，并于同日签署行政令，要求《TikTok 剥离法》在未来 75 天内暂不执行。

近几年，全球分工体系的变革和逆全球化思潮涌现兴起，地缘政治诉求的分裂和单向竞争加剧，使得企业在全球版图上的迁移成为监管和规制焦点，除了深层次的意识形态分歧外，来自文化和法规的冲

突具有更大的杀伤力，美国等国家的技术封锁、脱钩断供无疑为企业拓展海外市场增加更多障碍，对企业运营的障碍将以供应链安全风险的形式聚集，这将构成对全球可持续发展的重大隐患。

### 3. 网络安全形势严峻，各类攻击事件频发

2024 年，网络空间的攻击依然频发，高级勒索软件、人工智能驱动的网络攻击、供应链网络攻击等成为主要趋势，对能源网、医疗保健系统、供水/净水处理设施和交通网络等国家关键基础设施的网络攻击增加。典型如美国威立雅水务、英国南方水务先后遭遇勒索攻击、CrowdStrike 大规模蓝屏事件、黑客组织 IntelBroker 入侵欧洲警察署并窃取机密数据等。此外，俄乌冲突、巴以冲突依然没有结束，其“网络攻击战”依然在延续并有升级之势，例如，乌克兰黑客对俄罗斯电信运营商实施数据擦除攻击，乌克兰使用破坏性 ICS 恶意软件 Fuxnet 攻击俄罗斯基础设施，巴以冲突中以对中东部分国家能源基础设施实施的打击等。

为应对攻击，美国、荷兰、中国等国家的相关机构发布多个警报，提醒组织重视相关安全风险。美国 FBI 和 CISA 联合发布《DDoS 攻击可能会阻碍对选举信息的访问，但不会妨碍投票》公告，建议选民采取相关预防措施。CISA、FBI 和多州信息共享与分析中心（MS-ISAC）联合发布新版《了解和应对分布式拒绝服务攻击》指南，解决组织在防御 DDoS 攻击方面的需求和挑战。英国国家网络安全中心发布《网络安全评估框架（3.2 版）》，提出包括网络攻击防范在内的四个高级目标。中国国家计算机病毒应急处理中心发布《关于针对我国用户的“银狐”木马病毒出现新变种的预警报告》。中国工信部印发《工业控制系统网络安全防护指南》，提出 33 项指导性安全防护基线要求，防护对象包括工业控制系统以及被网络攻击后可直接或间接影响

生产运行的其他设备和系统。

针对勒索攻击后的赎金支付问题,《七国集团领导人普利亚公报》表示“为遏制不断增加的勒索软件攻击，将继续充分利用国际反勒索软件行动计划，并协调各方努力，避免支付赎金。”英国多机构发布《组织勒索攻击事件赎金支付指南》指出，受害组织在遭遇网络勒索时应谨慎决策、审查是否存在赎金支付的替代方案、记录决策过程、评估影响、调查事件的根本原因并向英国当局求助。指南指出，支付赎金会鼓励犯罪分子继续开展犯罪活动，英国国家网络安全中心不鼓励、认可或纵容组织支付赎金。澳大利亚议会批准的《网络安全法案2024》要求组织必须在72小时内报告向黑客支付的勒索赎金，并指出虽然不鼓励向网络犯罪分子付款，但在某些特殊情况下支付赎金是合理的。

针对安全事件的预防和处置，欧盟《网络安全条例》生效，旨在确保欧盟各机构、机关、办事处、部门采取共同的网络安全规则和措施搭建框架，提高欧盟机构内部网络安全恢复和事件响应能力。英国NCSC的《网络安全评估框架（3.2版）》也要求建立安全事件发生后全面分析机制，对组织程序问题以及网络、系统、软件中的安全漏洞进行分析。欧盟《网络团结法案》建立欧洲网络安全事件审查机制，对严重或大规模网络安全事件进行事后审查、评估，为如何提升欧盟网络安全水平提供建议。

2024年，中国国家安全部门公开发布境外间谍情报机关实施的网络攻击案件，揭发台湾资通电军下属网络战联队网络环境研析中心“匿名者64”的黑客活动。国家网络与信息安全信息通报中心发现诸多境外恶意网址和恶意IP，归属地主要涉及美国、波兰、荷兰、保加利亚、土耳其、日本等。

### 4. 网络安全合作紧密，全球公约正式发布

伴随着全球性网络安全威胁、攻击事件不断增多，各国在网络安全领域斗争与合作并存的趋势愈发明显。为了降低对抗的失控风险，共同应对价值共识下的网络安全挑战，维护网络空间安全与稳定，各国、区域间加强合作，并形成全球普遍适用的打击网络犯罪公约。

欧盟和加拿大共同启动新的《欧盟-加拿大数字伙伴关系》，重点加强人工智能、量子科学、半导体、在线平台管理以及网络安全方面的合作。捷克国家网络和信息安全局和以色列国家网络局签署网络安全谅解备忘录，旨在加强两国当局在网络安全领域合作，为双方提供交流网络安全最佳实践、分享网络安全重要信息的机会。英国科学、创新和技术部发布《英国和澳大利亚网络安全合作：谅解备忘录》，将加强合作，提升总体网络安全水平，强化对儿童、妇女等弱势群体的网络安全保护。芬兰、德国、爱尔兰、日本、波兰、韩国已加入由美英澳等 11 个国家组成的联盟，签署《关于努力打击商业间谍软件扩散和滥用的联合声明》。

12 月，联合国发布由 193 个成员国通过的《联合国打击网络犯罪公约》，是由中国、俄国等金砖国家倡导并引领推动，在广大发展中国家持续努力下促成的，也是国际社会首次就网络犯罪打击达成的一项具有全球性法律约束力的公约。《公约》超越了 20 多年前的 2001 年“欧盟版”《网络犯罪公约》，对网络空间国际法发展有重要的指标性意义。

## （二）关基安全保护规则持续细化，实践应用日益深化

面对变乱交织的国际形势和日趋严峻的网络安全态势，保障关键信息基础设施（以下简称“关基”）的安全弹性依旧是各国网络安全

保障的重中之重，外国势力、勒索攻击、人工智能等新技术在安全威胁中的应用、物理破坏等都成为各国关键信息基础设施安全保护的考量因素。美国国家网络主任办公室发布的首份《2024 年美国网络安全态势报告》表示，“美国关键基础设施面临着不断演变和不可接受的网络风险。民族国家的对手正在发展网络能力并获得访问权限，以破坏或摧毁美国及其盟国的关键基础设施。”CISA 表示“涉及关键基础设施的网络事件会迅速蔓延至相互依赖的基础设施，甚至影响公众”。同时，多国网络安全机构均指出诸多关键基础设施并未为未来的网络安全风险做好准备。如五眼联盟网络安全机构发布的《关键五国适应不断变化的威胁: 关键五国保障关键基础设施安全弹性的方法概要》报告中表示“许多关键基础设施对未来没有做好准备”。CISA 的网络安全咨询委员会（CSAC）发布的《构建关键基础设施弹性》报告草案指出“除少数例外情况，关键基础设施和政府机构尚未为国家冲突造成的竞争环境做好准备。”澳大利亚网络和基础设施安全中心发布的第二版《关键基础设施年度风险评估》报告也认为“大部分行业仍未达到网络素养和意识的基本水平。”

2024 年，以美国、欧盟、中国在内的主要国家和地区在关基安全保护的政策立法及安全实践方面持续推进，延续、更新、细化保护规则，深化关键基础设施内涵，强调风险发现和安全评估，并进一步加强行业、国家间协调配合。

## 1. 规则体系塑造稳步推进，重要保护思路延续

美国延续《2023 年国家网络安全战略》思路，对其中涉关键基础设施安全保护要求进行拆解并明确具体实施要求。2023 年 7 月发布的《国家网络安全战略实施计划 1.0》提出的 69 个启动项目在战略实施第一年已经完成 33 项；2024 年 5 月发布《国家网络安全战略实

施计划 2.0》，较 1.0 新增 31 项实施举措，新增内容聚焦供应链风险、勒索软件威胁、软件漏洞、公私合作等方面。

欧盟及其成员国 2024 年在关键基础设施保护方面的重要立法任务之一是推动 NIS 2 指令的转化与实施。欧盟委员会发布 NIS 2 指令首个实施条例，围绕 DNS、云计算、数据中心、内容分发等 11 类服务提供商提出细化的网络安全风险管理方法、技术措施和重大事件认定标准；成员国层面，根据 NIS 2 指令要求，成员国应当在 2024 年 10 月 18 日前将其转化为国内法。比利时是第一个全面实施 NIS 2 指令的成员国，克罗地亚、意大利、立陶宛也分别通过法令、网络安全立法等方式完成转换。11 月，欧盟委员会向剩余 23 个成员国发出正式通知函，要求其在两个月内完成转换。此外，马来西亚《2024 年网络安全法》及其四部配套条例正式生效施行，明确国家关键信息基础设施（NCII）行业、监管部门职责及实体义务，并通过建立许可制度规范网络安全服务提供商市场准入。

为进一步适应网络安全威胁形势，时任美国总统的拜登签署《关于关键基础设施安全和韧性的国家安全备忘录》（NSM-22），取代 2013 年发布的《总统政策指令——关键基础设施安全性和弹性》（PDD-21），细化和明确国土安全部及 CISA、行业风险管理机构等联邦政府机构在关键基础设施安全、弹性和风险管理方面的角色和责任，重申 16 个关键基础设施部门。备忘录授权国土安全部领导联邦政府关键基础设施安全保护工作，CISA 作为关键基础设施安全弹性协调员应在行业资源支持、风险评估、国际合作等方面发挥作用。备忘录发布后，国土安全部、CISA 等机构发布多项战略计划或指南文件，从强化国际合作、明确优先事项等视角落实备忘录要求。其中，国土安全部发布的《美国关键基础设施安全弹性战略指南和国家优先

事项（2024—2025 年）》明确关键基础设施行业应关注的五大优先风险领域和四项风险缓解措施。

近几年，关基保护体系在顶层立法层面已趋于成熟，其影响力正深刻渗透并细化至具体行业领域，形成更为精细且针对性强的规则下沉策略。以美国和中国为典型代表，两国均将顶层战略或者立法的原则与规范延伸至诸如交通、水利、电力等关键行业领域。交通运输行业，美国发布《关于修订保护美国船舶、港口和海滨设施相关法规的行政令》，赋予海岸警卫队应对网络安全事件的七项权限，并指示其发布关于海上运输系统网络安全的拟议规则制定通知，建立最低网络安全要求，强化海事领域网络安全保护。为落实该行政令，美国海岸警卫队和国土安全部联合发布拟议规则制定通知《海上运输系统网络安全》，表示海岸警卫队将制定网络安全计划，明确网络安全组织架构、确定网络安全官（CySO），进行网络安全演习，测试美国旗舰船舶、设施相关人员在履行分配的网络安全职责、落实网络安全计划方面的熟练程度。美国运输安全管理局发布拟议规则《加强 Surface 网络风险管理》，要求铁路、管道及高风险客运运营商制定全面的网络风险管理计划，建立监控和报告机制，并与 CISA 共享网络安全事件信息。中国交通运输部公布《铁路关键信息基础设施安全保护管理办法》，围绕铁路关基认定、运营者责任和义务、保障和监督等方面作出规定。

供水和废水行业方面。针对美国水务设施多次受到网络攻击，危及关键基础设施安全的现实情况，美国 CISA、FBI 和环境保护署联合发布《供水和废水行业事件响应指南》《保护水系统安全的顶级网络行动》，指出供水和废水行业网络安全事件响应应当包括事前准备－检测、分析－控制、源头治理、恢复－事后留痕四个环节，并提出

减少接触面向公众的互联网、定期网络安全评估、更改默认密码、盘点技术资产、系统备份等一系列行动措施。

电力方面，中国国家发展和改革委员会发布《电力监控系统安全防护规定》，从产品和服务安全漏洞管理、专用安全产品管理等方面对电力监控系统安全防护提出要求，并明确国家能源局及其派出机构的行政执法权。国家能源局印发《电力网络安全事件应急预案》，指导电力行业及时响应及处置安全事件。

## 2. 关基设施内涵动态调整，认定工作持续开展

明确关基内涵和范围是准确开展安全保护工作的前提。中国自《网络安全法》《关键信息基础设施安全保护条例》施行以来，各行业稳步推进关基认定工作。随着数字化转型的推进、基础设施间互联互通程度的提升以及网络安全形势的深刻变化，关基的内涵也随之调整变化。五眼联盟网络安全机构发布报告表示，尽管五眼联盟成员国对关键基础设施的定义可能略有不同，但近十年来关键的潜在共性并没有发生重大变化，仍继续使用以部门为基础的分类方法。部分国家还额外确定关键基础设施子部门，或优先考虑特定的重要资产和系统，以建立更全面的保护。

英国政府将英国数据中心归类为“关键国家基础设施”（CNI），这是自 2015 年太空和国防部门被认定为 CNI 以来，近十年首次获得 CNI 称号的机构。英国数据中心存储着在英国生成的大部分数据，将数据中心与水、能源和紧急服务系统放在同等地位，意味着数据中心能够在重大事件中恢复和预测方面得到政府更大的支持。澳大利亚内政部将 46 个关键基础设施资产指定为“国家重要系统”。“国家重要系统”是《2018 年澳大利亚关键基础设施安全法》引入的概念，旨在进一步确保澳大利亚最重要的关键基础设施安全。目前，已有

200 余项资产被列为“国家重要系统”，覆盖能源、通信、交通等多个领域。出于国家安全考虑，该清单并未对外公布。此外，美国在 NSM-22 号备忘录中提出“系统重要性实体”概念，指示 CISA 根据行业风险评估、跨行业风险评估等情况形成系统重要性实体清单，且该清单也不对外公布。

### 3. 风险发现仍是关注重点，事件报告更为精细

一是强调风险评估。美国 NSM-22 号备忘录要求行业风险管理机构每两年开展一次特定行业风险评估，确定行业最重要的关键基础设施风险。2024 年 6 月，CISA 发布行业特定风险评估指南，使用基于场景的方法将企业风险管理最佳实践应用于关键基础设施风险环境，并整合一系列定性和定量输入的最佳可用信息，以识别和评估国家面临的最大风险。

2024 年，CISA 共计发布近 1300 个网络防御警报、建议和产品，还持续开展现场演习，2024 年组织开展的 Cyber Storm IX 演习帮助关键基础设施测试和提高美国对重大网络事件的复原力、响应和恢复能力。Cyber Storm IX 演习借鉴了民族国家构成的网络安全威胁类型，包括影响关键基础设施的基于云的漏洞[1]。其中，将红队测试作为评估风险的重要手段之一。CISA 应要求对关键基础设施实体进行红队评估。根据 11 月发布的评估结果发现经评估的组织没有采取足够的技术控制措施来防止和检测恶意活动，领导层也错误地降低了内部安全团队发现的漏洞处理优先级及漏洞利用的潜在影响；基于上述经验教训，CISA 对组织及软件制造商提出安全建议，包括为用户提供定期培训、优先实施更加现代化的零信任网络架构、敦促软件制造商将安全嵌入整个软件开发生命周期的产品架构中等。在澳大利亚网络与

[1] [1] CISA 2024 Year in Review. https://www.cisa.gov/about/2024YIR

基础设施安全中心针对国家重要系统（SoNS）发布的《强化网络安全义务：网络安全演习指南》指出，演习可以不同形式进行，包括：（1）讨论和桌面演习，团队或个人讨论拟如何应对网络安全事件并探讨事件期间相关安全问题；（2）操作、功能演习，团队或个人模拟实施风险管理计划、流程和程序，预演网络安全事件发生时的各自角色和职责。

二是细化事件报告要求。为落实美国 2022 年 3 月《关键基础设施网络事件报告法》，CISA 发布拟议规则《〈关键基础设施网络事件报告法〉报告要求》。CISA 还上线专门的门户网站，并提供资源，指导并帮助实体报告网络事件。在欧盟委员会发布的 NIS 2 指令首个实施条例中也给出了重大事件的认定标准，考量因素包括是否影响商业秘密安全、自然人生命健康、系统中断以及造成的经济损失、事件发生频率等，并围绕 DNS、云计算、数据中心、内容分发等 11 类服务提供商给出更加具体的认定标准。

与之类似，中国密码管理部门 2024 年 11 月开始征求意见的《关键信息基础设施商用密码使用管理规定（征求意见稿）》围绕密码使用这一核心机制，给出了以密评为基础安全措施，密码人员配置和事件报告等为支持的关基风险控制思路。

### 4. 拓展多元化的合作路径，深化国际合作关系

关基安全事关国家安全，仅依靠单一国家或机构难以形成全面有效的安全保护体系，需要国家间、行业间持续强化安全协作。

一是政府部门特别关注资源匮乏的关基行业，加强指导和联系，缩小安全差距。2024 年，对于 CISA 认为“几乎没有资源投资于安全和弹性，已经成为攻击者理想目标”的水务和废水、教育、医疗保健和公共卫生服务部门，CISA 持续加强与上述部门的合作，通过发布

事件响应指南、工具包、成立协调和咨询机构、制修订网络安全绩效目标等方式提升关键基础设施行业安全。

二是国际合作更加密切。美国 CISA 和国家情报总监办公室发布《保护关键基础设施，保持警惕至关重要》，帮助关键基础设施所有者和运营商发现并缓解外国情报机构对美国关键基础设施的破坏行为。美国 CISA 发布首个综合战略计划《2025—2026 年国际战略计划》，提出增强美国所依赖的外国基础设施弹性、加强集成网络防御、协调国际活动三大战略目标。同时，关键基础设施保护仍然是各国深化伙伴关系、加强国际合作的重要内容。

近年来，以联合国、G20 为代表的多边组织在关基发展与安全上亦增加了大量共性认识，包括对数据基础设施的普遍接受，人工智能带来的关基风险，以及应通过发展，包括安全能力建设，以建立各国具有“复原力”的关键基础设施等等。

## （三）数据安全政策立法蓬勃发展，安全与发展导向深度调整

2024 年，数据安全依然是全球网络安全法治重点，数据安全制度、规则建设持续推进。包括数据安全在内的数据法治成为深度影响新一轮数字科技革命和产业变革乃至全球数字竞争的重要因素，各国数据政策立法安全与发展取向深度调整，数据法治体系在数据安全保护的基础上愈加充盈，作为数字经济立法的数据立法进一步发展，以促进技术进步与法治变革的良性互动。数字竞争、地缘政治等因素持续深度影响全球数据安全法治态势，随着对数字贸易需求的认知增加和经济增长的迫切需求，数据跨境的便利性和安全性如何协调，仍是各国数据安全政策立法的重中之重。以人工智能技术为代表的新一轮信息技术变革带来数据安全风险持续引发关注并导致部分既有政策法律的失效，各国开始积极探索、建立人工智能中的数据安全监管规

则。

### 1. 数据安全制度逐渐走向精细化，重点规则持续探索完善

围绕数据安全领域突出问题，各国相继发布安全管理细则。例如针对人脸数据，德国数据保护机构发布《安全卫生机构使用人脸识别系统的决议》，明确安全卫生机构使用人脸识别系统的限制条件；澳大利亚信息专员办公室发布《面部识别技术：隐私风险评估指南》；法国数据保护机构发布《货车内部增强型摄像头使用指南》。针对员工数据，德国联邦劳工和社会事务部和联邦内政部发布《员工数据法案（草案）》，明确员工数据处理规则和安全保护要求。针对数据匿名化，韩国个人信息保护委员会和科学与信息技术部发布《教育领域假名化和匿名化信息处理》指南。针对数据泄露，美国联邦通信委员会更新版《数据泄露通知规则》生效。

中国数据安全规范体系建设快速发展。国家层面，网络数据安全领域首个行政法规《网络数据安全管理条例》出台，弥补了中国数据治理领域全位阶法律规范体系中“行政法规”的缺失，为三法框架下的制度衔接与协调、规则细化与补充提供了解决方案，也为贯彻落实“坚持高质量发展和高水平安全良性互动”理念提供了重要范式。国务院审议通过《公共安全视频图像信息系统管理条例（草案）》，重点规范公共场所建设公共视频系统、采集视频图像信息的行为，进一步明晰各方责任，加强统筹管理、分类监管。

行业领域层面，《互联网政务应用安全管理规定》《自然资源领域数据安全管理办法》《会计师事务所数据安全管理暂行办法》《银行保险机构数据安全管理办法》相继发布，为政务应用网络与数据安全、自然资源领域数据安全、金融领域数据安全等提供重要规范。以民航局发布的《民航数据管理办法（征求意见稿）》《民航数据共享

管理办法（征求意见稿）》，国家邮政局发布的《寄递服务用户个人信息安全管理办法（征求意见稿）》等为代表的大量数据安全规则仍在制定中。

此外，工信部先后发布《工业和信息化领域数据安全风险评估实施细则（试行）》《工业和信息化领域数据安全事件应急预案（试行）》，为工业和信息化领域数据安全风险评估、应急预案制定提供具体操作指南。上海、天津相继发布《临港新片区数据跨境流动分类分级管理办法（试行）》《中国（天津）自由贸易试验区企业数据分类分级标准规范》，为数据安全制度的落实提供具体指引。

## 2. 安全与发展导向深度调整，数据利用政策立法蓬勃发展

随着新一轮科技革命和产业变革深入发展，数据作为关键生产要素的价值日益凸显。推动数据要素高水平应用，培育发展数据生产力成为各国数据法治重要导向。自欧盟 95 指令以来，个人数据保护问题始终在各国网络安全政策立法框架占据重要地位，特别是在 GDPR 之后，各国几乎对其予以全面复刻并不断进行改良、调整和细化。近年来包括欧盟、英国在内的诸多监管者已开始重新审视 GDPR 的制度设计并完善数据治理方案。经过几年时间的探索与调整，2024 年，全球数据法治体系在数据保护的基础上愈加充盈，促进数据流通利用规则建设持续、深入推进。破除数据流通使用堵点，实现数据资源向数据资产转变，助力构建与数字生产力发展相适应的生产关系成为诸多国家政策立法重点。

国际层面，欧盟《数据法》生效，作为促进欧盟数据流通规则，《数据法》赋予用户更广泛的访问权并明确终端用户有权在云和边缘服务提供商之间有效切换，以促进数据共享与再利用。为推进《数据法》实施，欧盟委员会先后发布《〈数据法〉常见问题解答》《〈数

据法〉解释指南》。

2024 年中国全面贯彻新发展理念，以“数据是新的生产要素，是基础性资源和战略性资源，也是重要生产力”为指导，持续部署、推进数据要素市场化配置改革，出台一系列政策、规定，为数据要素高质量供给、合规高效流通利用提供政策与制度支撑。一是激发供数动力。中共中央办公厅、国务院办公厅印发《关于加快公共数据资源开发利用的意见》，明确指出各级党政机关、企事业单位依法履职或提供公共服务过程中产生的公共数据，是国家重要的基础性战略资源，提出共享、开放、授权运营三种公共数据资源开发利用方式。国家数据局等五部门联合印发《关于促进企业数据资源开发利用的意见》，明确企业在生产经营过程中形成或合法获取、持有的数据，是企业发展的重要资源，并从健全企业数据权益实现机制、培育企业数字化竞争力、赋能产业转型升级、服务经济社会高质量发展、营造开放透明可预期的发展环境等方面提出具体措施。二是打造用数生态。国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》，提出实施可信数据空间能力建设、开展可信数据空间培育推广行动、推进可信数据空间筑基三大行动计划。国家发展改革委等部门印发《关于促进数据产业高质量发展的指导意见》，提出加强数据产业规划布局、培育多元经营主体、加快数据技术创新、提高数据资源开发利用水平、发展数据流通交易、强化基础设施支撑、提高数据领域动态安全保障能力、优化产业发展环境等九大举措。三是探索建设数据基础制度、规则。国家发展改革委发布《公共数据资源登记管理暂行办法（公开征求意见稿）》，国家数据局发布《公共数据资源授权运营实施规范（试行）（公开征求意见稿）》。《数据领域常用名词解释（第一批）》首次对数据、原始数据、数据资源、数据产品与服务、数据资产等数

据领域常用名词定义作出统一解释。

### 3. 数据跨境安全仍是重点关注，规则不确定性依然突出

跨境数据流动已成为数字经济的关键推动因素，数据跨境传输依然是各国关注重点。欧盟委员会通过《加拿大与欧盟间转移和处理PNR数据协议的提案》，《欧盟－日本跨境数据传输协议》正式生效，巴西数据保护机构发布《数据传输条例》和标准合同条款，沙特数据与人工智能管理局发布《个人数据跨境传输条例》《个人数据跨境传输标准合同条款》等多项个人数据跨境新规和指南。中国不断优化数据跨境流动安全管理制度。国家顶层持续部署促进数据依法有序流动，扩大高水平对外开放。国家网信办出台《促进和规范数据跨境流动规定》，对数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境安全管理制度作出优化调整。天津、北京自由贸易试验区数据出境管理清单（负面清单）相继发布。上海临港新片区发布《数据跨境场景化一般数据清单》，为数据跨境传输开展了有益探索。此外，国家网信办与澳门特别行政区政府机构签署《关于促进粤港澳大湾区数据跨境流动的合作备忘录》，有力促进了内地与澳门之间的数据传输。

与此同时，基于国家安全、国际竞争、隐私保护等诸多因素，数据跨境流动面临诸多现实挑战，国家、地区间数据跨境流动规则仍未形成共识，部分国家将数据问题泛安全化，针对特定国家差别化制定数据跨境流动限制性政策，实施歧视性的限制、禁止等措施，阻碍数据跨境流动，也为数据跨境带来了诸多不确定性。如美国发布《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据行政令》以及《防止受关注国家或涵盖人员访问美国敏感个人数据和政府相关数据的规定》的最终规则，以国家安全为由限制美国敏感个

人数据或美国政府相关数据向中国、俄罗斯等国家传输。中国发布《全球数据跨境流动合作倡议》，阐明中国在全球数据跨境流动问题上的立场主张，以数字贸易的便利性与安全性平衡构建新型多边数据跨境规制，推动既有的“古早”规则适时调整，将成为未来双边、多边协定中贸易规则设计、谈判的焦点。

### 4. 人工智能安全风险突出，数据安全监管规则持续探索

人工智能已经成为新一轮科技革命和产业变革的重要驱动力量，也是大国竞争的重要领域。欧盟、新加坡、韩国等纷纷加强战略部署试图在新一轮的国际竞争中占据先发优势。与此同时，以海量数据收集与处理为运行基础的人工智能尤其是生成式人工智能的数据与隐私保护问题进一步凸显。围绕人工智能的新问题，各国多结合技术进路和各自国情展开探索。如何在促进人工智能技术创新与发展的同时保护数据安全与隐私成为各国人工智能治理的重要考量。

欧洲数据保护监督机构（EDPS）发布《生成式人工智能数据合规指引》，为欧盟机构使用生成式人工智能系统处理个人数据提供实操建议和指南。新加坡个人数据保护委员会发布《隐私增强技术：合成数据生成拟议指南》，协助组织了解合成数据生成技术及其应用场景（特别是人工智能领域），以及生成合成数据时应采用的良好实践，实现隐私保护和保障数据质量之间的平衡。韩国个人信息保护委员会发布《人工智能开发和服务中公开数据处理指南》，为企业合法、安全地处理人工智能开发和服务中所收集、利用的公开数据提供标准。

2024 年 7 月，中国的全国人大常委会法制工作委员会进一步阐述了人工智能立法的思路：一是优先考虑灵活适用现有法律规则，通过法律解释或司法解释，解决人工智能发展过程中面临的突出法律问题；二是对于某些人工智能应用的具体场景，可以通过授权立法的方

式，由地方在立法权限范围内先行先试；三是针对影响产业发展的痛点难点问题，在迫切需要法律予以规范的领域，坚持“小快灵”立法原则，通过修改现行法律的方式解决。

## （四）个人信息保护立法不断完善，执法力度持续强化

个人信息政策立法在国际环境的复杂性与不确定性中不断演进、持续完善，执法力度不断强化。同时，地缘政治影响个人信息跨境流动规则，人工智能等新技术持续冲击个人信息保护的传统规则。

### 1. 保护规则精细化趋势明显，法律贯彻实施力度加强

全球个人信息或者隐私保护专项立法制定修订频繁。智利、埃塞俄比亚等国家颁布首部个人数据保护基本法，填补本国在该领域的立法空白，全球拥有统一个人数据保护制度的国家群体进一步壮大。部分国家紧密贴合个人信息保护新形势和新需求，及时调整、优化已有立法，典型如，澳大利亚皇室批准《2024 年隐私和其他立法修正案》，修订《1988 年隐私法》以落实政府在回应《1988 年隐私法》审查报告时所承诺的首批改革措施。马来西亚通过《个人数据保护法（修正案）》，修订 2010 年《个人数据保护法》，增加强制数据泄露通知义务，将生物识别数据纳入敏感个人数据，加大处罚力度等。以色列通过《隐私保护法（修正案）》，强化隐私保护机构的监督执法权力，减少数字信息数据库的注册义务降低监管负担等。土耳其通过《个人信息保护法（修正案）》，对敏感个人数据处理以及个人数据跨境传输等方面进行修订。智利官方公报公布《个人数据保护法》，以使其个人数据保护水平接近欧盟 GDPR 以及其他拉美个人数据保护先进国家的标准和水平。

同时，欧盟、英国、美国等个人数据保护或隐私保护立法先行地

区或者国家持续细化、完善个人信息保护规则。欧盟持续推进 GDPR 适用和执法一致性工作。欧盟数据保护委员会发布《2024—2025 年工作计划》，围绕四大支柱提出关键行动，包括针对 GDPR 的关键问题和概念制定进一步指导方针，支持制定和实施针对控制者和处理者的合规措施，针对欧盟个人数据保护方面的重要问题向欧盟立法机构提供建议等。欧盟网络安全局发布《欧盟数据空间中个人数据保护工程》报告，强调欧洲数据空间中个人数据保护的设计原则。

美国犹他州通过有关特殊领域、特殊主体个人信息保护的立法。其中，《机动车消费者数据保护法》对联网或“智能”车辆供应商管理作出要求和限制，《社交媒体监管修正案》要求社交媒体平台对未成年人账户实施年龄验证和家长控制，《访问受保护健康信息》澄清第三方请求提供医疗记录或付款和余额信息所涉及的个人权利和义务。加利福尼亚州发布首份针对《加州消费者隐私法》的执法建议《将数据最小化应用于消费者请求》，将数据最小化作为 CCPA 的一项基本原则，防范未经授权的数据访问活动。

韩国持续发布相关指南，强化个人信息保护合规指引，包括《假名信息处理指南（修订）》《个人信息处理政策评估通知》《公共机关提供假名信息实务指南（21.1）》《海外企业个人信息保护法适用指南》《处理人工智能（AI）开发和服务中使用“公开数据”标准指南》《数据主体自动化决策指南》《移动型影像信息处理设备个人信息保护指南》等。

中国《网络数据安全管理条例》进一步完善细化个人信息保护要求。国务院发布《消费者权益保护法实施条例》，对经营者的个人信息保护义务作出规定。国家邮政局发布《寄递服务用户个人信息安全管理办法（征求意见稿）》，规范寄递企业用户个人信息处理活动。

公安部、国家互联网信息办公室等发布《国家网络身份认证公共服务管理办法（征求意见稿）》，旨在实施网络可信身份战略，强化公民个人信息保护。国家标准层面，《数据安全技术 基于个人请求的个人信息转移要求（征求意见稿）》《数据安全技术 个人信息保护合规审计要求（征求意见稿）》《网络安全标准实践指南——敏感个人信息识别指南》等相继发布。

执法方面，欧盟及其成员国围绕 GDPR 的执法持续活跃。其中，爱尔兰数据保护委员会因职业社交平台 LinkedIn 违反 GDPR 规定，将用户个人数据用于行为分析和定向广告，对其处以 3.1 亿欧元罚款，是 2024 年度 GDPR 执法中最高的一笔罚款。美国个人信息与隐私保护相关执法力度进一步强化。州层面，得克萨斯州检察长与 Meta 达成 14 亿美元的和解，原因是 Meta 在未经用户授权的情况下使用个人生物识别数据。该和解结束了得克萨斯州总检察长在 2022 年向州法院提起的诉讼指控，即 Meta 在未经德克萨斯民众同意的情况下对上传到 Facebook 的照片使用面部识别软件。韩国大力推进《个人信息保护法》实施，个人信息保护委员会因未经许可处理个人敏感信息对 Meta 处以 216 亿多韩元（约合人民币 1.12 亿多元）的行政罚款。

## 2. 数据跨境流动格局演变，影响个人信息出境规则

全球数据跨境流动格局不断演变，各国有关数据跨境流动规制的分歧进一步凸显，部分国家调整个人信息跨境传输规则。欧盟在 GDPR 构建的数据跨境传输机制下持续完善个人信息跨境传输示范合同条款，支持不同合同类型下标准合同条款（SCCs）规则的应用。2024 年，欧盟通过了从处理者到处理者的个人数据传输示范合同条款，并计划对另一套 SCCs 进行公开咨询，以解决向直接受 GDPR 管辖的第三国控制者和处理者进行数据传输的问题。除欧盟外，其他多

个国家也发布了标准合同条款。如，巴西数据保护机构（ANPD）发布第 19/2024 号决议，批准《数据传输条例》和标准合同条款。沙特数据与人工智能管理局（SDAIA）发布《个人数据跨境传输标准合同条款》。土耳其个人数据保护机构（KVKK）发布特定类型数据传输的标准合同条款。

美国数字主权与国家安全意识形态进一步强化，数据跨境立场进一步从“自由流动”向“自由流入、严格流出”演变。2 月，拜登政府依据《国际紧急经济权力法》（IEEPA）发布一项保护美国人个人敏感数据免遭“关注国家”利用的行政命令，确立“禁止受关注国家获取包括美国公民敏感个人数据在内的数据”的立场。对此，美国司法部发布执行该行政命令的拟议规则制定的预通知并持续推进相关事项，并于 12 月通过《应对外国对手获取美国公民敏感个人数据的最终规则》。该规则禁止数据经纪商向中国、古巴、伊朗、朝鲜、俄罗斯和委内瑞拉等国家，以及特定被列为“受限人员”的个人和实体，提供美国人的个人敏感数据。

马来西亚对个人信息跨境传输规则进行调整，其通过《个人数据保护（修正案）》取消 PDPA 授权部长发布个人数据跨境传输目的地国家白名单的规定，允许数据控制者在目的地国家存在与 PDPA 基本相似的现行法律或者至少具备与 PDPA 相当保护水平的情况下跨境传输个人数据。

中国基于数据出境安全评估、个人信息出境标准合同备案等制度实践中发现的问题，对数据出境规则进行优化。《促进和规范数据跨境流动规定》针对个人信息出境规定了免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形，同时提高个人信息出境适用数据出境安全评估的门槛，减轻企业个人信息出

境合规负担。《网络数据安全管理条例》则在吸收《促进和规范数据跨境流动规定》针对个人信息出境豁免情形的基础上新增“为履行法定职责或者法定义务，确需向境外提供个人信息”豁免情形。随着中国探索数据跨境流动的便利化，《粤港澳大湾区（内地、澳门）个人信息跨境流动标准合同实施指引》《网络安全标准实践指南——粤港澳大湾区（内地、香港）个人信息跨境处理保护要求》相继发布，粤港澳大湾区个人信息跨境流动便利机制基本成型。

执法司法方面，荷兰数据保护局因违反 GDPR 规定将欧洲地区司机的个人数据跨境传输至美国且对相关数据保护不足，对美国网约车服务运营商 Uber 公司处以 2.9 亿欧元罚款。因违反韩国《个人信息保护法》第 28（8）条关于跨境传输个人信息规定以及第 31（2）条和第 38 条关于难以行使数据主体权利的规定，韩国个人信息保护委员会对阿里巴巴全球速卖通处以 19.78 亿韩元（约合 143 万美元）罚款和 780 万韩元（约合 5640 美元）滞纳金，责令改正并提出改善建议。中国公开发布第一起个人信息跨境传输法院判例。该案系某国际酒店因将消费者个人信息提供给境外加盟酒店以及合作伙伴进行处理而引发的纠纷。案中，某国际酒店超出“履行合同所必需”范围，基于营销目的将原告个人信息传输至境外实体，但仅通过简单勾选一揽子隐私政策获取用户同意，被法院认定不满足《个人信息保护法》单独同意的要求，进而判决其向原告赔礼道歉、删除原告全部个人信息并赔偿财产损失 2 万元。

### （五）供应链安全政策立法持续发展，各环节规则日臻完善

当前，供应链安全已成为网络安全风险重要来源，提升供应链韧性和安全是全球主要国家或地区的重点关注。美国将保障供应链安全作为国家重大经济发展战略。推动供应链重塑是拜登政府核心政策之

一，先后发布《确保国家供应链安全》《关于改善国家网络安全》等行政令并成立供应链中断工作组，强化供应链安全审查和风险监控。《欧洲经济安全战略》将供应链弹性风险列为当前欧盟经济安全领域主要存在的四大风险之一，并持续通过立法强化供应链安全保护制度体系。中国也高度重视供应链安全。党的十八大以来，习近平总书记多次对产业链供应链安全稳定作出重要指示，强调“要把增强产业链韧性和竞争力放在更加重要的位置，着力构建自主可控、安全高效的产业链供应链”。

### 1. 强制性立法与参考性指引结合，推进供应链安全治理

2024 年，各国监管对供应链安全治理紧迫性的认识不断深化，法治探索加速进行，包括硬法规制与软法规制两个方面。

硬法方面，美国发布《关于防止关注国家获取美国公民大量敏感个人数据和美国政府相关数据的行政命令》，以保障供应链安全为由，限制相关数据向特定国家传输。英国《2022 年产品安全和电信基础设施法》及相关条例生效，适用范围涵盖联网智能设备的制造商、进口商和分销商等供应链环节上的各方，明确联网智能设备的安全要求。欧盟《网络弹性法》正式生效，强化带有数字组件的产品安全保障。欧盟委员会通过《关键实体和网络安全实施条例》，要求相关实体应制定、实施和应用供应链安全政策，并对供应链安全管理提出具体要求。此外，英国政府宣布将推出《网络安全和弹性法案》，强化供应链安全是其中重要内容。中国《网络数据安全管理条例》对网络数据安全的关注不再是节点安全而是整个产业链供应链的安全问题。在规则设计上，对供应链安全提出特别要求，包括供应商安全风险告知、报告义务，政务或类政务系统供应链安全管理要求等。

软法层面，以美国为代表的国家发布一系列供应链安全配套指南，

为行业提供具体指引。美国国家标准与技术研究院（NIST）发布网络安全框架（CSF）2.0 版，这是该框架十年来的首次重大更新。CSF 2.0 极大扩展适用范围，从关键基础设施领域扩大到所有组织，并重点关注治理和供应链问题。CISA 发布《构建软件组件透明度：建立通用软件物料清单》，提供每个软件物料清单属性的最低预期、推荐做法和理想目标。NIST 发布 NIST SP800-161r1-upd1《系统和组织网络安全供应链风险管理实践》指南，对包括企业在内的组织所面临的供应链风险提出指导建议，识别、评估和缓解跨组织层面的供应链网络安全风险。此外，CISA、FBI 还与澳大利亚网络安全中心合作，发布针对软件制造商和服务业的指南《安全软件部署：软件制造商如何确保客户可靠性》，帮助制造商实施全面测试和安全软件部署，以增强产品及其部署环境安全性。

## 2. 重视供应链各环节安全，强调开源软件安全可靠

供应链覆盖产品或服务的设计、开发、生产、采购、交付等诸多环节，供应链安全也相应覆盖各个环节安全。欧盟《网络弹性法》对硬件和软件产品的设计、开发、生产和在市场上提供均提出了要求。此外，采购是网络产品、服务提供者等主体融入网络运营者供应链的重要途径，同样是有效防范引入新的供应链安全风险的重要环节。要求将网络安全因素纳入采购考量、设置采购安全标准、摸清供应商底数等手段成为各国强调采购环节安全保障要求的立法选择。美国 CISA 等部门发布《网络供应链风险管理生命周期中的软件保障》《按需安全指南：软件客户如何推动安全的技术生态系统》，通过为供应链中的采购方提供安全指引，引导其将安全纳入供应商要求以提升供应链安全。此外，突破合同自由原则，明确供应商合同应规定安全义务条款成为各国采购要求之一。无论美国总统行政令还是欧盟《网络

弹性法案》均要求把供应链安全保障义务纳入双方合同，并呈现将供应链安全从关基领域延伸到“价值供应”和其他领域的泛化趋势。

与此同时，全球新一轮的产业数字化升级对开源软件的依赖日益提升，强化开源软件管理成为各国供应链安全管理的重要内容。4 月，以色列隐私保护局发布的《在数据库系统中使用开源代码的信息安全风险管理指南》，对组织使用开源代码并将其集成到系统中的实践提供安全指导；为降低开源代码带来的信息安全风险，指南建议在纳入开源代码之前采取代码审计等措施。6 月，美国 CISA、FBI 与澳大利亚网络安全中心以及加拿大网络安全中心联合发布指南《探索关键开源项目中的内存安全》，为软件制造商提供创建内存安全路线图的初始框架，特别强调处理外部依赖项中内存安全问题的战略规划。8 月，CISA 和 FBI 发布《按需安全指南：软件客户如何推动安全的技术生态系统》，要求软件制造商应当维护和共享第三方依赖项的来源数据，并建立相应流程以管理开源软件组件。软件采购方应当审查软件制造商是否以标准且机器可读的格式生成软件物料清单并向客户提供，包括开源软件。

### 3. 各国供应链安全监管强化，安全评估成为重要手段

安全评估是发现供应链安全风险的重要手段之一。欧盟正式生效的《网络弹性法》要求制造商对数字产品进行网络安全风险评估，并在产品规划、设计、开发、生产、交付和维护阶段考虑评估结果。中国《网络数据安全管理条例》也明确要求处理重要数据的大型网络平台服务提供者报送的风险评估报告，应当充分说明关键业务和供应链网络数据安全等情况。以色列隐私保护局发布《在数据库系统中使用开源代码的信息安全风险管理指南》，建议在纳入开源代码之前采取评估风险，评估开源代码可能带来的具体风险，并制定应对措施。

5 月 9 日，澳大利亚网络安全中心、美国 CISA、加拿大网络安全中心、英国国家网络安全中心和新西兰国家网络安全中心联合发布指南《选择安全且可验证技术的安全设计》，明确在考虑采购产品或服务时，采购方还应对自身进行评估。在采购前、中、后三个阶段，采购方均应就采购过程的政策、基础设施、安全问题等咨询组织高级管理层，并根据其意见实施采购活动。美国国防部向管理和预算办公室提交《评估承包商对网络安全要求的实施情况》的提案，要求对承包商遵守网络安全要求的情况进行评估，此项计划旨在落实《2020 财年国防授权法》第 1648 条规定，核心目标是为国防工业基础部门建立一个基于风险的网络安全框架。CISA 和 FBI 发布《按需安全指南：软件客户如何推动安全的技术生态系统》，建议在软件采购生命周期的各个阶段融入安全考虑，从采购前评估软件制造商的安全策略，到合同中纳入安全要求，再到采购后的持续安全评估。

中国也在一些重要行业、领域推动对 ICT 供应链的更新认知和标准工作。如国家金融监督管理总局发布《银行保险机构数据安全管理办法的通知》，强调银行保险机构应对外部数据供应商进行安全管理，统筹大数据应用、数据共享项目的安全需求管理；供应链服务中涉及敏感级及以上数据处理的，银行保险机构应当加强对供应商的准入和安全管理，延续了以网络数据分类分级为基础的安全保护理念。

### 4. 全方位加强特殊主体监管，未成年人保护尤其突出

2024 年，特殊类型、特殊场景、特殊主体的个人信息保护问题持续受到监管关注，儿童/未成年人个人信息保护尤其突出。针对儿童个人信息与隐私保护的执法力度持续加大。美国司法部代表 FTC 对 TikTok 及其母公司提起诉讼，指控其违反美国《儿童在线隐私保护法》以及其与 FTC 在 2019 年达成的关于儿童隐私的和解协议。英

国信息专员办公室针对儿童在线保护问题，对 34 个社交媒体和视频共享平台进行审查，并特别要求 11 家公司解释与默认隐私设置、地理位置或年龄保证相关的问题，并展示采取的方法如何符合准则。巴西数据保护局发布第 50/2024/FIS/CGF/ANPD 号技术说明，就处理未成年人数据不遵守《通用数据保护法》行为要求对 TikTok 采取纠正措施并开始制裁程序；发布 29/2024/FIS/CGF 号决定，禁止 X 使用未成年人数据训练人工智能。

美国联邦层面着力推进《儿童在线安全和隐私法案》《儿童在线安全法案》，旨在强化对儿童和青少年的保护，要求社交媒体平台采取更多措施来防止未成年人接触有害内容，并限制对其个人数据的收集和使用。科罗拉多州签署《儿童在线数据隐私保护法》，规定如果存在对未成年人造成伤害的高度风险时必须进行数据保护评估，禁止出售未成年人个人信息或是进行定向广告。纽约州通过《儿童数据保护法》，规定禁止企业未经同意收集 18 岁以下未成年人的数据，并限制出售未成年人数据等。澳大利亚通过《2024 年隐私和其他立法修订法案》，引入与儿童在线隐私、自动决策和数据泄露相关的条款。中国《未成年人网络保护条例》设立专章对未成年人个人信息保护作出规范。

新加坡、西班牙、波兰等国家相关机构发布儿童个人信息保护指南。新加坡 PDPC 发布《关于数字环境中儿童个人数据的咨询指南》，阐明《个人数据保护法》如何适用于儿童个人数据在线处理活动。西班牙数据保护局发布指南《儿童默认安全上网和年龄验证的作用》，切实做好儿童保护工作。波兰数据保护局发布指南《互联网上的儿童形象：是否应该发布》，旨在确保机构和组织在数字时代更好地保护儿童。阿根廷发布《我们的数字世界指南》，强调未成年人在个人数

据保护方面的权利。

### 5. 人工智能治理关注个人信息，通过立法明确保护要求

技术进步和市场需求共同推进人工智能的多元化发展和应用，个人信息与隐私保护问题在各国人工智能治理的政策立法中得到进一步强调。欧盟在统一规制的立法进路下，通过《人工智能法》强调在人工智能系统的开发和应用中保护个人隐私的重要性，将“隐私和数据治理”纳入人工智能系统开发、使用的六项原则之一。欧盟数据保护监督机构发布《生成式人工智能数据合规指引》，指导欧盟机构遵守《关于欧盟机构、机关、办公室和代理处在处理个人数据时保护自然人以及此类数据自由流动的条例》，针对生成式人工智能场景下的数据保护提出一系列基本要求。

美国联邦层面尚未通过综合性人工智能立法。科罗拉多州《与人工智能系统互动中的消费者保护法》关注与人工智能交互中的消费者保护，要求高风险人工智能系统开发者采取合理谨慎措施，避免高风险系统中出现算法歧视。犹他州《人工智能政策法》从透明和非歧视地使用人工智能方面对消费者权益保护作出规定。

英国、澳大利亚、巴西等也针对人工智能中的个人信息与隐私保护问题作出规定。英国中央数字与数据办公室发布《英国政府生成式人工智能框架》，要求组织在使用生成式人工智能工具时应当确保其安全性，包括确保在没有数据所有者知情或同意情况下，不会使用私人或敏感数据源来训练生成式人工智能模型等。澳大利亚信息专员办公室发布《关于隐私以及开发和训练生成式人工智能模型的指南》，指导使用个人信息训练生成式人工智能模型的开发人员遵守隐私保护要求；发布《关于隐私和商用人工智能产品使用的指南》，指导组织选择合适的商用人工智能产品，并在使用时履行隐私保护义务。巴

西数据保护局发布《人工智能应用法（修正草案）》，明确在人工智能系统决策背景下个人享有的基本权利，包括对人工智能系统的决策提出异议并要求服务商提供解释，特定情况下要求人工介入算法决策过程，获取人工智能系统运行信息，不遭受人工智能系统的歧视并要求系统纠正歧视性偏见等。

中国秉承将个人信息与隐私保护作为人工智能健康发展内在要求的立场，《网络数据安全管理条例》针对人工智能的数据训练提出针对性条款，亦有中法共同发布《中华人民共和国和法兰西共和国关于人工智能和全球治理的联合声明》，中俄《关于深化新时代全面战略协作伙伴关系的联合声明》等，强调个人数据、人工智能用户权利保护等问题。全国网安标委发布《生成式人工智能服务安全基本要求》，提出服务提供者需遵循的安全基本要求，其中对使用个人信息作为训练数据、处理个人信息等方面提出明确要求。

## （六）信息内容治理成为关注焦点，各国侧重有所不同

算法和人工智能技术的迅速发展，不仅重塑了信息生成与传播的全链条，而且触及社会结构的深层肌理，给网络生态治理带来深刻变革和严峻挑战，持续引发全球范围内的广泛关注。从国际视角观察，欧美国家展现出对涉政虚假信息及儿童信息保护问题的特别重视。中国则展现出更为宽广的视野与更为全面的考量，在同样重视儿童信息保护的基础上，还关注网络暴力、网络谣言、网络水军等问题。

### 1. 未成年人受到广泛关注，相关立法执法活动加强

当前，网络发达国家的未成年人群网络普及率非常高。互联网已经全面融入未成年人的学习和生活，并超越电视成为未成年人获取信息的最广泛渠道。保护未成年人上网安全，保障未成年人网络信息权

益，是世界各国共同努力的方向。

加拿大政府发布《网络危害法案》，针对欺凌儿童、教唆儿童自残、未经同意发布色情内容等 7 类网络有害内容进行监管，要求各大社交媒体平台须在 24 小时内删除涉及儿童的违规帖文。澳大利亚皇室批准《2024 年在线安全修正案（社交媒体最低年龄）法》，要求存在年龄限制的社交媒体平台（如 Snapchat、TikTok、Facebook、Instagram、X 等）采取合理措施，禁止 16 岁以下的未成年人创建账号，保护未成年人免受社交媒体带来的潜在心理健康风险和网络犯罪威胁，违反规定的社交媒体平台将面临最高可达 4950 万澳元（约合 2.3 亿元人民币）的罚款。英国通信管理局发布《儿童安全实务守则（草案）》，要求内容推荐算法运营商、搜索引擎服务提供商等行业企业采取有效的年龄检测和评估技术、有效的算法过滤技术、建立健全内容审核机制等措施保障儿童上网安全。

中国国家互联网信息办公室发布《移动互联网未成年人模式建设指南》，面向移动智能终端、移动互联网应用程序、移动互联网应用程序分发平台，提出未成年人模式建设的总体方案，具体包括使用时段、时长、内容和功能等方面，适用于未成年人模式的研发、建设、运营和管理。中央网信办开展的“清朗·2024 年暑期未成年人网络环境整治”专项行动，累计清理拦截涉未成年人违法不良信息 430 万余条，处置账号 13 万余个，关闭下架网站平台 2000 余个，从严处置各类危害未成年人身心健康的“毒视频”、集中整治针对未成年人的“开盒挂人”乱象、严厉打击隔空猥亵等网上恶性违法犯罪行为、深入整治网上涉未成年人违规售卖问题、排查下架一批涉未成年人违规应用活动。

## 2. 全球大选加速虚假信息传播，涉政虚假信息治理成为重点

2024 年，全球 50 多个国家和地区举行约 70 次大选，这也是各国首次在生成式人工智能被广泛应用的环境下进行的选举周期，网络涉政虚假信息问题成为影响选举安全的核心议题。随着对视频、图片、音频进行深度伪造的技术更加成熟且普遍，造假的成本也更加低廉，引发国际社会对深度伪造的强烈不安。联合国区域间犯罪和司法研究所指出，日益普遍化、平民化的生成式人工智能工具可生成冒充知名公职人员的可信虚假内容，显示政客收受贿赂等，导致社会骚乱、抗议和选举中断，而深度伪造视频发布的时间节点至关重要，如选举最后一天。

美国、欧盟、新加坡等主要国家和地区在 2024 年大选期间对生成式人工智能的应用与管控为观察新技术对政治、法治的影响提供重要实例。如何区分生成内容与真实内容，如何评估模型生成欺骗性选举内容相关的安全风险，如何推进事实核查标签与生成内容水印体系，如何提高公众批判性人工智能素养与技能（分析复杂现实、认识观点与事实之间的差异以及生成式人工智能相关风险）成为各国治理重点。

欧盟委员会 2024 年 1 月宣布，对即将到来的成员国和欧盟层面的选举等活动，要求 17 家超大型在线平台（VLOP）和超大型搜索引擎（VLOSE）授权研究人员访问平台数据，以便监测在线平台非法内容。3 月，欧盟委员会根据《数字服务法》第 35（3）条规定，出台《关于超大型在线平台和超大型在线搜索引擎提供商缓解选举过程系统性风险的指南》，要求 VLOP 和 VLOSE 采取提供官方选举进程、提升公众媒体素养、提供用户核查信息途径、阻断有害信息等措施，减轻选举安全相关系统性风险。新加坡立法机关通过《2024 年选举（在线广告完整性）（修正案）法案》，禁止操纵以候选人深度伪造

为特征的在线选举广告。

在 Sora 发布的第二天，OpenAI、亚马逊、谷歌、微软、TikTok、Facebook 母公司 Meta、社交平台 X 等全球多家领先的科技企业签署《打击在 2024 年选举中欺骗性使用人工智能的技术协议》，承诺在这一特殊年份，通过技术部署减少利用生成式人工智能生成、分发欺骗性内容干扰选举的风险。随后，联合国发布《全球数字契约：零案文》呼吁科技公司继续开发人工智能生成内容识别、内容真实性认证和溯源、水印等技术。加拿大、法国、德国、意大利、日本、英国和美国七国集团（G7）外长以及欧盟高级代表共同发布《七国集团外长 2024 年意大利会议关于应对全球挑战、加强伙伴关系的声明》，强调人工智能在外国信息操纵和干预中的作用，呼吁社交媒体平台加大力度防范并打击外国信息操纵和干预活动，降低人工智能技术滥用风险。

美国分别与芬兰、波兰签署《打击外国信息操纵谅解备忘录》，加强打击外国国家信息操纵合作，保护选举安全，避免破坏公众对政府的信任。美国国家情报总监办公室、FBI、CISA 联合发布《确保选举基础设施免受外国恶意影响行动指南》，重点讨论外国恶意影响行动中使用的策略并提供解决方案，包括提高选举透明度，加强公职人员社交媒体账号安全管理，提升选民和员工的信息安全意识等。

### 3. 信息内容治理规则更加细化，网络谣言依然是打击重点

中国一直重视网络生态治理工作。2024 年，中央网信办举报中心指导全国各级网信举报工作部门、主要网站平台畅通举报渠道，加大违法和不良信息受理处置力度，受理处置网民举报线索 2.27 亿件，同比增长 10.4%。在网络信息内容治理中，网络暴力、网络谣言是重

点打击对象，国家互联网信息办公室、公安部、文化和旅游部、国家广播电视总局联合发布《网络暴力信息治理规定》，这是一部典型的事件驱动型立法，涉及预防预警、信息和账号处置以及保护机制等内容。

中央网信办、公安部在打击谣言、网络暴力、网络水军等方面取得重要成果。中央网信办深入推进“清朗”系列专项行动，集中开展违法信息外链、‘自媒体’无底线博流量、网络语言文字使用等十个重点领域的整治活动。各级网信部门执行专项行动要求取得一系列进展。公安部党委将2024年作为打击整治网络谣言专项行动年，部署全国公安机关开展为期一年的专项行动，打防管控一体推进，持续加大全链条、全平台、全领域打击力度。

针对扰乱社会公共秩序的造谣传谣类违法犯罪活动，公安机关深入开展打击整治网络谣言专项行动，依法严惩网红大V、MCN机构有组织造谣炒作，2024年侦办网络谣言案件4.2万余起，查处造谣传谣违法犯罪人员4.7万余人，关停违法违规账号33万余个，清理网络谣言信息252万余条。针对通过网络实施侮辱谩骂、造谣诽谤、侵犯隐私等违法犯罪活动，持续开展打击整治网络暴力违法犯罪专项行动，侦办网络暴力案件8000余起。针对造谣引流、舆情敲诈、刷量控评、有偿删帖等突出网络水军违法犯罪活动，坚持重拳出击、露头就打，侦破案件1000余起。此外，军地职能部门针对网络涉军谣言进行依法依规处置，就捏造军事谣言、杜撰军事史实、抹黑军队形象、曲解军事政策、煽动军地对立、消费拥军情怀等通报地方网信部门予以处置。

## 4. AI 为违法信息蔓延提供便利，各国执法部门严厉查处

美国国土安全部发布报告指出，生成式人工智能（例如深度伪造）为不法分子操控网络社交媒体提供了便利。互联网中渗透的大量虚假信息不仅迷惑网络用户，而且影响搜索引擎、平台流量算法。美国联邦通信委员会（FCC）和新罕布什尔州总检察长办公室同时发文称，对 1 月该州民主党初选期间，使用 AI 技术伪造拜登声音敦促选民“不要投票”的幕后操纵者，发动刑事指控和经济处罚的追责，本案也被视为美国“AI 干预选举第一案”。美国政府宣布成立一个跨部门特别工作组，旨在帮助公众识别数字内容（包括音视频、图片）如何以及何时被人工智能工具修改、生成或操纵。工作组将与国际政府和合作伙伴共同努力，推动技术透明度标准的制定，增强能力建设，并提高公众对人工智能驱动的数字内容的认识；除制定标准外，工作组还将推动实施针对官方政府制作的数字内容的透明度措施。

境内方面，重庆市梁平公安对康某某利用人工智能自动生成文章，编造重庆巫溪发生爆炸造成 4 人死亡的谣言，对其依法行政拘留；四川德阳公安对刘某群人工智能小程序自动编辑功能，嫁接为发生在德阳某学校的“校园霸凌”虚假信息依法处以行政处罚。随着人工智能技术的成熟，开发门槛逐渐降低，导致出现大量管理不严格的公司为违法犯罪活动提供了人工智能工具。重庆九龙坡区网信办依法对属地“开山猴”AI 写作网站运营主体重庆初唱科技有限公司未尽到审核管理义务、履行主体责任不到位的行为，依据《网络安全法》第六十八条规定，给予行政警告处罚，并责令该公司限期全面整改，加强信息内容审核，健全信息内容安全管理相关制度，暂停网站信息更新及 AI 算法生成式写作功能 15 日。

## （七）人工智能不同法治形态蓬勃发展，推动发展与安全的辩证统一

2024 年，以 ChatGPT、Copilot、Sora 等为代表的人工智能技术和工具进一步开发、迭代和广泛应用。同时，大国竞争、地缘政治等因素加剧人工智能领域政策立法博弈。当下面对的已经不是要不要发展人工智能，而是要发展什么样的人工智能、怎样发展人工智能以及如何适应人工智能时代的人机协同等问题。

### 1. 规范制定与技术发展同步，国际治理规则取得进展

每一项颠覆性技术的出现，均会对现行社会秩序甚至法律秩序造成一定冲击。对人工智能技术革命引发的新情况、新问题，全球法治探索呈现繁荣态势，且随着人工智能伦理、原则等软法难以满足实践需求，国家强制力保障的硬性立法逐步进入各国视野。全球首部人工智能综合性法律欧盟《人工智能法》正式施行，针对通用目的人工智能模型专门治理并规定有系统性风险的通用目的人工智能模型提供者的义务。各国人工智能立法探索步伐加快，韩国国会全体会议通过《旨在构建人工智能发展与信赖基础的人工智能基本法案》，加拿大推动《人工智能与数据法案》，日本制定《负责任的人工智能促进基本法案（暂定）》等。

2024 年以来，针对 ChatGPT 的数据与隐私监管执法活动在各国掀起热潮，司法方面围绕模型训练、输出是否侵权以及人工智能生成物是否受知识产权保护多起诉讼相继提起。欧盟委员会通过启动“人工智能协议”，以更好地推进欧盟《人工智能法》落地，并鼓励和支持企业预测和提前规划该法规定的合规措施。美国《关于安全、稳定和可信的人工智能行政令》指示 50 多个联邦机构执行 100 多项具体

行动，各机构已于2024年1月全部完成行政令指示的90日行动目标。中国国家互联网信息办公室根据《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》已发布累计九批境内深度合成服务算法备案信息。

人工智能安全国际治理规则的影响力外溢是技术发展和市场演变的客观进程，但这一进程也受到权力博弈的主动塑造。2024年人工智能安全治理国际合作取得一系列重要成果。联合国通过《抓住安全、可靠和值得信赖的人工智能系统带来的机遇，促进可持续发展》决议草案，鼓励采取有效措施，促进创新，以便在人工智能系统的设计和开发期间以及在部署和使用之前，对脆弱性和风险采取具有国际互操作性的识别、分类、评估、测试、预防和缓解措施。欧洲委员会正式通过首部具有法律约束力的人工智能国际条约《人工智能与人权、民主和法治框架公约》。七国集团（G7）签署《G7部长宣言：人工智能部署和创新》，探讨如何利用数字化转型和人工智能以包容、可持续的方式推动经济和社会发展。澳大利亚、美国、英国、加拿大、新西兰、德国、以色列、日本、挪威、新加坡、瑞典等十一国联合发布指南《与人工智能互动》，为组织安全使用人工智能系统提供指导。五眼联盟国家网络安全机构联合发布指南《安全部署人工智能系统》，提供部署、运行人工智能系统的最佳实践。新加坡和澳大利亚签署一份新的谅解备忘录（MOU），重申两国致力于促进公民和组织采用人工智能，并推动负责任的人工智能开发部署。

## 2. 精细化场景化趋势明显，重点规制高风险应用

在产业应用上，大模型从基础设施层趋向细分应用并通过高通量、低门槛、高自由度的生成能力赋能办公、交通、医疗等多行业、多场景，大模型应用生态迅速壮大并蓬勃发展。各国关注通用目的人工智

能系统和模型的潜在风险，同时兼顾政务、公共事务等重点应用。美国国土安全部发布《2024 年国土安全部人工智能路线图》，强调在负责任使用人工智能推进国土安全任务的同时，保护个人隐私、公民权利和自由，明确未来发展目标。鉴于人工智能与警务等场景固有特性的融合交叠容易诱发执法权的固有属性被侵蚀、潜在偏见传导放大、公民基本权利遭侵犯等风险，美国、欧盟、加拿大、英国等针对大模型技术发展强化对预测性警务的管控。国际刑警组织和犯罪司法所发布《新版执法领域人工智能负责任创新工具包》，为执法机构在尊重人权和伦理原则的同时负责任开发、部署人工智能提供指南。

此外，人工智能用于军事武器、医疗保健、网络安全、关键基础设施等领域等最紧迫的安全风险受到关注，在组织机构设置、应急处置、风险评估与披露等方面提出要求。联合国通过《军事领域人工智能和国际和平及安全》，确认国际法适用军事领域人工智能，旨在促进人工智能技术的正当和有效利用。美国白宫发布《推进国家安全领域人工智能治理和风险管理的框架》，指出“高影响”人工智能使用情形包括设计、开发、测试、管理或停用可能无意中成为武器的敏感化学或生物、放射性或核材料、装置或系统等。世界卫生组织发布《医疗健康人工智能伦理与治理：大型多模态模型指南》，概述 40 多项建议供政府、技术公司和医疗健康提供者参考。

### 3. 风险分类分级成为共识，治理动态包容性凸显

人工智能应用风险实际是技术创新对原有技术、经济、社会平衡关系的冲击所带来的。在技术、经济、社会都处在动态变化的情况下，人工智能安全监管不再是静态制度实施过程，提升人工智能安全治理和监管的动态适应性，是对人工智能技术、经济、社会动态变化所引发的利益相关者之间复杂利益冲突做出的主动性监管制度的应然回

应。欧盟《人工智能法》以风险分级、分类治理为核心理念,将人工智能应用风险分为四级差异化监管，并针对类 GPT 大模型引入通用目的人工智能专门条款。具体而言，被划分为不可接受风险的，禁止其进入市场并进行应用；被划分为高风险的，要求开发者应采取严格的监管措施，并在投放市场之前以及在产品运营的整个生命周期内接受安全评估；被划分为有限风险的，则要求其必须遵循透明度原则，评估和减少可能的风险，并在欧盟市场发布前应在欧盟数据库中进行注册；被划分为低或轻微风险的，不列入监管范围。着眼于更广阔的数字立法浪潮，《人工智能法》与《通用数据保护条例》《数字市场法》《数字服务法》《数据法》《数据治理法》等协同联动。

为贯彻落实《全球人工智能治理倡议》，中国全国网络安全标准化技术委员会发布《人工智能安全治理框架》，按照风险管理的理念，紧密结合人工智能技术特性，分析人工智能风险来源和表现形式，针对模型算法安全、数据安全和系统安全等内生安全风险和网络域、现实域、认知域、伦理域等应用安全风险，提出相应技术应对和综合防治措施，以及人工智能安全开发应用指引。制定中的《网络安全等级保护条例》也提出，网络运营者应当按照等保制度要求，管控人工智能等新技术、新应用带来的安全风险。

### 4. 创新发展成为各国核心诉求，法治与战略竞争密切耦合

智能体、智算集群、高质量数据集、具身智能等成为 2024 年以来人工智能创新发展的关键词。本阶段全球人工智能立法的探索与实践，是在国际体系深度调整、国际格局加速演变的特殊背景下进行的。在全球主要经济体增长放缓背景下，大模型等颠覆性技术是全球经济未来一段时间可带来全局效应的少有增长点。大国战略竞争赋予大模型安全治理以及战略稳定以特殊路径和方向。对内，各国抢先布局，

通过政策立法营造有利发展环境，支持重点领域人工智能研发、税收优惠鼓励企业创新，探索研发、开源模型豁免规则以及监管沙盒机制等，促进本国大模型产业发展，维护自身技术领先优势和国家利益。对外，算力、算法、数据、模型等关键资源成为竞争焦点，美欧出口管制和安全审查的重点从半导体、先进芯片制造设备拓展到云计算、开源大模型等领域。美国白宫发布有史以来首份关于人工智能的国家安全备忘录《关于推进美国在人工智能领域的领导地位、利用人工智能实现国家安全目标，促进人工智能的安全、安保和可信性的备忘录》，凸显美国管控国家安全领域人工智能特殊风险、利用前沿人工智能技术赋能美国国家安全保护、制裁对手国家人工智能能力发展、围绕人工智能推动国际共识及治理等多重战略意图。

伴随人工智能带来的弥散性影响紧密交织、叠加拓展，人工智能供应链安全风险态势能力建设的重要性凸显，供应链安全评估、设计安全、安全反馈等成为各国战略关注点。澳大利亚等十一国联合发布《与人工智能互动》，重申《安全人工智能系统开发指南》重要性，强调人工智能供应链安全评估有助于识别、管理风险，若组织参与训练人工智能模型，也应将基础训练数据和微调数据供应链纳入考量，防范数据中毒，确保数据和模型参数安全。在人工智能语境下，“设计安全”不仅意味着在选择内部开发还是使用外部组件时将供应链安全纳入考量，还应将模型开发融入现有的安全开发和最佳实践中，关注系统开发生命周期风险管理、深度防御、建立漏洞标识等，针对人工智能对抗性输入，注重保护底层系统和模型。此外，各国已意识到保持开放沟通渠道、获得人工智能安全反馈的重要性，鼓励安全研究人员研究、报告漏洞，美国国防部等相继开展人工智能赏金计划。

监管互操作性、通用性成为各国人工智能法治探索中的重要考量。

各国已然意识到，在制定人工智能监管标准时，不仅要考虑国内适用，也要考虑全球其他国家的监管情况，通用可行的制度规范和产业标准有助于推动引导本土人工智能产业创新发展。以加拿大《人工智能和数据法（草案）》为例，尤其注重监管标准的国际互操作性，引入人类监督和监控、透明度、公平公正、安全性、可归责性、有效且稳健等与国际规范保持一致的原则和措施，旨在推动加拿大人工智能产业链上下游积极开展全球布局。

综上，不同国家、地区的人工智能法治包含不同的结构和要素，塑造不同的法治形态，产生不同的法治效应，形成不同的生成、演进和发展逻辑。人工智能技术发展不会从根本上改变法治，但会改变法治状态；法治不能从根本上改变技术发展，但可影响技术发展进程，塑造未来的产业生态、权力构造、价值分配。伴随各国人工智能法治实质化进程加速推进，法治竞争的影响力日益提升，人工智能的法治选择是否与技术发展规律相契合、能否产生高质量治理效能，也会影响各国在人工智能战略竞争中的成败。

## （八）网络安全基石作用日益凸显，密码相关政策法律加速推进

全球数字化转型加速背景下，重要国家和地区的密码法治持续施行、调整、优化和完善，一方面凸显创造更安全的网络空间和数据流动环境、更有利的贸易促进措施赋能各国数字经济发展的特点，另一方面，也呈现出基于密码技术尤其是后量子密码（PQC）提升国家安全保障能力及竞争优势的特点。2024 年全球范围内对抗量子密码的关注和布局保持平稳上升态势，多国政府、国际组织相继行动，推动量子密码的研发、应用及其标准化进程，尤其关注量子计算对现有加密体系的潜在威胁，强调向后量子密码迁移的紧迫性，并基于抗量子密码作为先进技术的两用物项属性，在进出口监管（如量子计算、抗

量子密码技术出口管制）、国内产业促进（向后量子迁移协调、建立行业同盟）等方面体现出内外有别的整体政策立法特点。

### 1. 密码法律制度不断健全，规则更为细化和明确

2024 年，密码使用、出口管制、协助解密、电子认证等重要制度在前期基础上不断完善、更新、迭代。美国 CISA 发布《加密 DNS 实施指南》，澳大利亚信号局（ASD）更新《信息安全手册—密码学指南》，强化密码使用。欧盟持续侧重协助解密义务，欧盟委员会小组发布“关于有效执法数据获取的建议”主席报告，强调供应商合作解密义务。中国坚决贯彻落实《密码法》《商用密码管理条例》，加速商用密码重要制度的制定和迭代，部署全国范围内的商用密码使用和密评等监督检查，发布《电子政务电子认证服务管理办法》，推动制定《关键信息基础设施商用密码使用管理规定》，工业和信息化部牵头修订《电子认证服务管理办法》。国务院公布《两用物项出口管制条例》，贯彻落实总体国家安全观，建立统一高效、适用于商用密码的两用物项出口管制制度。

### 2. 安全基石作用日益凸显，网络安全立法明确密码合规要求

2024 年，密码的安全基石作用日益凸显，国内外网络安全立法纷纷明确密码产品和密码应用等要求。欧盟《网络弹性法》将身份管理系统软件、密码管理器等产品纳入该法规制范围。CISA 根据美国第 14117 号行政令的指示，提出数据安全拟议规则，提议使用同态加密或差分隐私等技术，以防止敏感数据被反向重构。西班牙数据保护机构将加密系统应用评估作为在线数据合规工具。中国《网络数据安全管理条例》《铁路关键信息基础设施安全保护管理办法》《自然资

源领域数据安全管理办法》《电力监控系统安全防护规定》《互联网政务应用安全管理规定》等，均强调落实密码应用要求，《国家网络身份认证公共服务管理办法（征求意见稿）》要求公共服务平台的建设和服务涉及密码的应当符合要求。江苏、湖南、浙江等地有关网络安全、数字经济促进的地方性法规，如《湖南省数字经济促进条例》《广东省数据条例》等均要求落实密码应用。

### 3. PQC 标准化制标进展重大，深刻影响科技创新与产业生态

2024 年 8 月 13 日，美国 NIST 正式宣布推出全球首批三项后量子密码标准 FIPS 203、FIPS 204 和 FIPS 205，引起国际社会普遍关注。历时八年取得后量子密码标准化制标工作的重大成果，进一步凸显了美国争夺量子霸权的战略企图。NIST 后量子密码标准化取得的此次重大进展，表明美国在全球后量子密码规则制定和迁移实现中已抢占先机，并在延缓乃至避免量子计算机对现有公钥加密机制的破解中取得领先优势。三个标准的正式发布是对未来量子计算威胁的一种前瞻性防御，对各国技术路线选择、科技创新与产业生态、技术主张和价值偏好等方面都将造成重要影响。

中国有关行业和企业都在积极探索后量子密码的应用和布局。2024 年，中国网安标委发布《全国网络安全标准化技术委员会 2024 年度工作要点》，提出研制密码相关标准，推进 PQC 算法等新国际标准提案立项。中央网信办、市场监管总局、工业和信息化部联合印发《信息化标准建设行动计划（2024—2027 年）》，布局开展量子计算、量子通信、量子测量等关键技术标准研究。

### 4. PQC 迁移依然是核心议题，具体实施呈现多样灵活性

2024 年度 PQC 迁移依旧是各国关注的焦点，以路线图、建议、

报告、倡议等灵活性方式推动迁移。欧盟委员会发布《向 PQC 迁移的协同实施路线图建议》，鼓励成员国制定统一战略，确保不同成员国及其公共部门之间向 PQC 的协调和同步迁移，包括明确的目标、关键里程碑和时间表，以实现保护欧盟公共管理部门数字基础设施及其他关键基础设施服务的目的。奥地利、比利时、丹麦、法国、荷兰等 18 个欧盟成员国的网络安全机构联合发布《保护明天、今天：向后量子密码学过渡》的声明，强烈建议在大部分用例中部署融合了 PQC 和传统加密方法的混合解决方案，并指出根据欧盟委员会建议，法国、德国、荷兰共同创建了 PQC 工作流，鼓励所有欧盟成员国在准备向后量子密码过渡的路线图过程中积极参与，以确保欧盟数字基础设施的量子弹性。

美国多个政府部门均重视向 PQC 的迁移过渡，白宫发布《PQC 学报告》，估计到 2035 年联邦机构向 PQC 学迁移将花费 71 亿美元以上的资金。同时，白宫下令开始评估国家安全在量子计算方面的准备情况。国家情报总监办公室发布《美国情报界信息环境展望：信息技术路线图》，明确情报界应当全面部署 PQC，确保最敏感情报数据安全。国家安全局设定 2035 年为集成电路系统遵守 PQC 标准的最后期限，以防止“先记录，后解密”等量子网络事件等。CISA 发布《迁移到自动化 PQC 发现和清单工具的策略》指南，建议联邦民事行政部门机构使用自动化 PQC 发现和清单工具进行初始系统清单，并尽快启动迁移流程。NIST 发布《向后量子密码迁移标准》的初始公开草案，提出迁移到后量子密码的路线和时间表。

英国信息专员办公室发布报告，指出各组织必须开始为向量子安全系统过渡做准备。爱尔兰教育与科研创新部发布其首个量子技术国家战略“量子 2030”，认为安全的量子通讯应当从量子密码、量子

计算基础架构、量子密钥分发和云安全的量子计算四个方面，这些共同构成向量子时代过渡的准备工作。英国国家网络安全中心发布年度回顾报告，敦促英国所有部门尽快迁移到 PQC，以确保出现量子计算威胁时能保护数字系统和数据的安全，并降低与 PQC 过渡相关的潜在网络风险。

澳大利亚内政部正在主导制定澳大利亚网络安全战略，包含到 2030 年实现澳大利亚成为全球网络安全领导者的发展路线图，其中明确涉及量子计算对当代密码学的潜在挑战，以及采用后量子密码标准的重要性。

荷兰情报与安全总局、荷兰国家数学和计算机科学中心以及荷兰应用科学研究组织联合发布第二版《后量子密码迁移手册》，阐述了向量子安全环境转型的最新进展和指导建议，涵盖如何识别加密资产、评估量子计算风险以及加强加密方法灵活性等实用指导。

### 5. PQC 领域国际合作持续深化，出口管制成为重要法律工具

2024 年量子科技、PQC 领域国际合作呈现出持续深化与蓬勃发展的态势。如美德政府签署联合声明，加强两国在量子信息科学与技术领域的合作。美国与捷克发布首届网络对话联合声明，指出双方将扩大双边合作，重点关注人工智能和量子技术，包括量子科学和量子计算研发领域，探索各自研究机构和产业双边合作的新途径。美国白宫政策办公室发布国家科学技术委员会量子信息科学小组委员会制定《推进量子信息科技领域的国际合作》报告，作为对《量子信息科学国家战略》的补充，为美国在量子信息科技领域的国际合作提供战略指导和政策建议。美国和新加坡在第二届美新关键和新兴技术对话中，重申双方将继续在量子安全迁移、密码资产迁移、量子安全产品安全保证等方面进行合作，并探索量子通信、计算和传感领域的合作

机会。

此外，北约发布首份《量子技术战略》，要点之一包括建立跨大西洋量子共同体。北约认为，量子就绪联盟成立需要盟国之间更紧密合作，构建有韧性的量子生态系统，一个量子就绪的联盟将能够更好地检测和阻止网络空间的潜在入侵。七国集团网络专家组（CEG）发文，就网络安全政策问题向七国集团财政部长和央行行长提出建议，鼓励各司法管辖区监测量子计算的发展，促进相关公私部门利益相关者之间的合作，并着手应对量子计算对现有加密方法的威胁。

在欧盟，比利时、保加利亚和波兰宣布签署《欧盟量子技术宣言》，至此欧盟 27 个成员国中已有 21 个签署该宣言。该宣言致力于在整个欧洲建立起世界级的量子技术生态系统，将欧洲打造为世界的“量子谷”，成为全球量子卓越和创新的领先地区，这也将是欧盟“数字十年”的主要优先事项之一。该宣言就多项量子问题在成员国之间达成协议，包括通过开展各项活动深入了解量子技术对社会和经济的影响，以及量子计算可能给当前加密技术带来的挑战。

中国国家主席习近平在亚太经合组织第三十一次领导人非正式会议上指出，要抓住新一轮科技革命和产业变革机遇，在人工智能、量子信息、生命健康等前沿领域加强交流合作，营造开放、公平、公正、非歧视的创新生态，推动亚太地区实现生产力跃升。

与此同时，出口管制成为 PQC 技术竞争中的重要法律工具。出口管制历来是保持国家技术优势、战略优势乃至国家安全的有效手段。美欧正重新定位和修改量子技术、后量子密码出口监管规则。2024 年 9 月 5 日，BIS 发布一项临时最终规则，与其盟友一同对量子计算等关键新兴技术实施管制，未来还会通过“将对某些技术产品的全球分销方式进行规定”的方式加强量子计算出口管制。同日，欧盟委员

会宣布对《欧盟两用物项出口管制条例》附件一中所含的两用物项清单进行修订，将密码定义扩展为“可用或可变得可用”的加密，同时引入“加密激活”概念，通过定义扩张加密产品或服务的使用场景，对更多加密产品和服务进行更严格的控制和监管。

此外，加拿大出于国家安全考虑，宣布政府计划停止资助“指定研究组织”敏感技术领域的研究，密码学领域包括生物识别加密、PQC、同态加密等，“指定研究组织”包含中国、俄罗斯等国家的研究机构。法国政府通过一项关于量子计算机和量子技术以及先进技术设备相关货物和技术出口的新命令，自 2024 年 3 月 1 日起，从法国向非欧盟国家出口与量子计算机和半导体等先进电子元件相关的技术将需要获得法国双重用途管理局的双重用途服务许可证，受限制的设备和技术范围包括量子计算机和量子技术。荷兰政府发布军民两用物项的相关出口管制措施，将量子计算机、量子测量设备和量子芯片制造技术等八种类型的产品纳入出口管制范围，如果荷兰公司想在欧盟以外地区销售，需要获得出口许可证。

中国商务部、工业和信息化部、海关总署、国家密码局根据《出口管制法》《两用物项出口管制条例》有关规定，联合发布更新的《中华人民共和国两用物项出口管制清单》中，限制出口的物项包括“以量子力学和密码学为基础，利用量子技术实现密码功能的设备（量子密码设备）”。

## （九）虚拟货币全球监管格局形成，涉加密货币犯罪打击成热点

2024 年，全球虚拟货币监管格局发生重大转变，全球范围内虚拟货币监管治理加速推进。各国政府纷纷出台政策法律规范虚拟货币市场，同时也积极探索如何平衡监管与技术创新、金融安全以及保护能源等方面的关系，为虚拟货币未来发展奠定坚实基础。

## 1. 加密货币认可度提升，合法性议题立场多元

随着虚拟货币与传统金融体系联系渐密，境外普遍将虚拟货币纳入本地新经济发展战略，虚拟货币服务许可、加强金融消费者权益保护等成为监管的关键词。由于发展阶段、制度背景和监管动机不尽相同，各国针对虚拟货币交易是否合法等议题呈现出不同的取向，但均在促进金融创新与防范风险之间寻求平衡。

据美国智库大西洋理事会统计，[2]虚拟货币交易等活动在33个国家和地区合法，在17个国家和地区部分禁止，在10个国家和地区全面禁止。在12个G20国家和地区（占全球GDP的57%以上）中虚拟货币目前合法，所有G20国家和地区都在考虑对虚拟货币采取监管措施。研究发现，虚拟货币采用率与监管限制性之间是弱相关的，即使在部分或全面禁止虚拟货币的国家，采用率仍然很高。

特朗普在2024年大选中多次宣传积极支持加密货币发展的政策主张，表示将把比特币列为美国战略储备资产，美国政府“拥有将近21万枚比特币，占总供应量的1%”，“确保美国成为地球上的虚拟货币之都和世界上的比特币超级大国”，其根本出发点是强化美元在国际货币体系中的主导地位。12月，比特币策略研究所为特朗普政府起草了一份关于将比特币纳入美国战略储备资产的总统行政命令，建议设立战略比特币储备，纳入财政部外汇稳定基金。该命令主张将比特币视为“数字黄金”，以提升国家经济安全，巩固美国金融主导地位，并推动数字资产行业发展。

日本议员提议政府推出国家比特币储备，建议日本政府“考虑将部分外汇储备转换为比特币等虚拟货币”。日本金融厅发布文件，公

[2] Atlantic Council.Crypto regulation tracker.[EB/OL].[2024-11-05].https://www.atlanticcouncil.org/programs/geoeconomics-center/cryptoregulationtracker/.

布其在2025财年税收改革请求中的立场，希望开始将加密资产视为“普通公众可以投资的金融资产”。

欧盟全球首部综合性的虚拟货币监管法律《加密资产市场监管法》正式生效，规定只有在欧盟成员国之一设有注册办事处，并获得相关国家主管部门授权作为加密资产服务提供商的法人或其他经营者，才能提供加密资产服务。申请加密资产服务提供商应提供证明，明确管理机构成员及股东没有犯罪记录或反洗钱和反恐怖主义融资、欺诈有关的处罚记录。该法针对加密资产服务提供商提出许可证、储备金、透明度报告、发行限制、独立审计等要求。基于该法，欧盟宣布自2024年12月30日起，所有在欧盟境内运作的加密货币交易平台停止提供Tether公司发行的USDT稳定币的交易服务。

俄罗斯在入侵乌克兰后面临全球制裁，迫使其转向加密货币以规避制裁。俄罗斯通过《关于数字金融资产、加密货币及对某些法律法规的修改决定》《关于在实验性法律制度框架内进行数字货币跨境结算和交易所交易的法律》，使加密货币挖矿合法化，并为央行使用加密货币进行国际支付铺平道路。新法允许组织进行挖矿，个人在能源限额内无需注册即可挖矿。

韩国《虚拟资产用户保护法》生效，旨在保护加密货币投资者并规范韩国的虚拟资产市场。该法将数字资产定义为具有经济价值、可以电子方式交易或转让的电子代币，包括一般加密货币，不包括非同质化代币和央行数字货币。

巴哈马通过《2024年数字资产和注册交易所法》，旨在应对数字资产和加密货币市场不断变化的格局。该法为稳定币提供了明确定义，规定现有稳定币的注册和可接受的储备资产形式，并为储备资产的保管、隔离、报告和赎回建立了新的要求。发行算法稳定币被明确

禁止。

中国香港地区《证券及期货条例》《打击洗钱及恐怖分子资金筹集条例》生效，规定在香港经营业务或向香港投资者推广其服务的虚拟资产交易平台营运者的双重牌照制度。截至 2024 年 11 月，获得香港证监会（SFC）正式发牌的虚拟资产交易平台营运者有 2 家，为 OSL 数字证券有限公司及 Hash Blockchain Limited。

## 2. 关注能源消耗违法活动，因地施策限制非法“挖矿”

2024 年 11 月，俄罗斯一项新法律生效，显著扩大政府对全国加密货币挖矿活动和相关基础设施监管，根据地区需求对加密货币挖矿活动施加限制。该法使俄罗斯政府能够按地点实施采矿限制，并规定禁止采矿作业的具体程序和情况。该法将国家采矿登记的责任从数字发展部转移到联邦税务局。从 2025 年 1 月 1 日起，俄罗斯 10 个地区（达吉斯坦、印古什共和国、卡巴尔达-巴尔卡尔等）全面禁止加密货币挖矿，为期六年。俄罗斯还批准在主要加密货币挖矿地区进行季节性限制，以防止停电。2024 年 4 月，俄罗斯警方曾在西伯利亚四个大型“非法”数据中心的突袭中查获 3225 台加密挖矿设备，并对挖矿中心运营商提出刑事指控。据报道，矿工们从新西伯利亚电网窃取了总计价值 210 万美元的电力。

巴拉圭当局从非法运营商手中没收超过 10000 台 ASIC 矿机，没收的比特币挖矿设备数量与委内瑞拉相当。1 月—7 月，国家电力管理局在巴拉圭对涉嫌比特币挖矿的农场进行了 70 多次突击检查，旨在保护国家电网的安全和稳定。

中国北京市发展和改革委员会、北京市机关事务管理局等十二部门联合发布《北京市进一步强化节能实施方案（2024 年版）》，明确提出整治虚拟货币“挖矿”活动，加强“挖矿”活动监测分析、分

类整治，坚决依法依规清理本市虚拟货币“挖矿”活动。

### 3. 加密货币犯罪演变，反洗钱等犯罪防治探索

鉴于加密货币本质属性的模糊和监管不到位构成加密货币犯罪泛滥的重要原因之一，基于对加密货币本质的深入理解，逐步明确各自的监管职责和重点，强调既有法律和监管工具对加密货币及交易所的适用性、延展性是通常做法。美国众议院通过对加密货币治理有里程碑意义的《21 世纪金融创新与技术法案》，厘清证券交易委员会与商品期货交易委员会在加密货币监管中的角色与职责边界，解决加密货币作为证券或商品的分类争议，力求构建相对严格的加密货币交易平台监管框架和交易规则。该法案已经提交给参议院，鉴于特朗普所在的共和党同时掌控了参议院和众议院，为立法进程提供了有利的政治环境，就此而言该法案最终获得通过的可能性有所提升。

惩处层面，各国执法部门加大对利用虚拟货币等洗钱犯罪的打击力度，并探索为警方在扣押、冻结和销毁犯罪分子使用的加密资产方面提供授权。美国司法部一向注重打击涉加密货币犯罪生态，将起诉、逮捕加密货币犯罪分子以追究其责任作为首要任务，同时摧毁犯罪基础设施，剥夺犯罪经济利益，没收非法所得并返还受害者。2021 年 1 月，美国《银行保密法》适用范围扩大至虚拟货币领域，2024 年执法力度持续加强，美国加密货币期货交易所 Digitex Futures 创始人兼 CEO 亚当·托德在美国联邦法院认罪，承认公司未构建反洗钱计划，违反《银行保密法》。

英国《经济犯罪和企业透明度法》加密资产相关规定生效，为应对近年来毒贩、诈骗分子和恐怖分子等有组织犯罪者越来越多地利用加密资产进行洗钱和资金筹集等问题，授权执法机构可以没收用于犯罪的加密货币，使英国执法部门更容易有效调查、扣押和追回非法加

密资产。澳大利亚联邦议会通过《2024 年犯罪和其他立法修正案（综合第 1 号）法案》，在《刑法》中插入数字资产定义，明确与场所相关的有效搜查令，授权执行官员或协助警察扣押数字资产的具体情形。

德国萨克森州虚拟货币保管与处置中心与法兰克福的专业证券交易银行 Scheich Wertpapierspezialist AG 合作，在联邦刑事警察局的支持下，完成约 49858 枚比特币的出售，收入约为 26.39 亿欧元，这是德国首次如此大规模进行比特币的紧急出售。

新加坡发布《新加坡反洗钱执法策略》，提出强化追踪和追回虚拟资产的能力，明确新加坡警察部队已制定《加密货币搜查与扣押标准作业程序》，对所有新加坡警察部队的调查人员开展相关培训。越南国家副总理签署《打击洗钱、资助恐怖主义、资助大规模毁灭性武器扩散国家行动计划》，旨在强化虚拟资产监管，履行越南政府与金融行动特别工作组共同预防和打击洗钱、恐怖主义融资的承诺。

中国境内继续强化对虚拟货币交易的禁令，全面禁止的监管思路在 2024 年的立法、司法解释及刑事案例中进一步强化。最高人民法院、最高人民检察院联合发布《关于办理洗钱刑事案件适用法律若干问题的解释》，将“通过虚拟资产交易、金融资产兑换方式，转移、转换犯罪所得及其收益的”行为，明确列为《刑法》第一百九十一条第一款第（五）项规定的“以其他方法掩饰、隐瞒犯罪所得及其收益的来源和性质”。十四届全国人大发布《反洗钱法（修订草案二次审议稿）》，对 2007 年施行的《反洗钱法》进行首次重大修订，将应对涉虚拟货币等新型洗钱风险涵盖在内。另一方面，虚拟货币的财产属性在司法实践中得到认可，相关主体持有虚拟货币具有合法性。

## （十）网络犯罪链条打击共识初步形成，首部具备普遍法律约束力的全球性国际公约通过

在互联网、物联网、大数据、云计算、元宇宙、人工智能等各种信息网络技术迭代升级背景下，犯罪分子利用大模型、加密货币等进行犯罪辅助，犯罪纵向精细切割，横向分工细化，交错而成利益链条，形成复杂的网络犯罪生态，呈现泛罪名化、泛技术化、泛组织化、泛产业化、泛地域化等特点，给社会安全治理带来诸多挑战。各国已然意识到，仅依赖刑事手段打击网络犯罪远远不足，亟需多层面、多角度强化犯罪防范、打击与治理。

### 1. 坚持利益链条打击，以整合性应对碎片化

网络犯罪泛滥蔓延的重要原因之一是在利益驱使下存在大量为网络犯罪提供帮助、寄生获利的黑灰利益链条，不铲除“输血送电”的利益链条，就无法从源头上遏制网络犯罪，需要从个案规制走向生态治理，从单个环节转向全链条、全流程规制。2024 年，新加坡通信和信息部发布《保护新加坡人免受网络诈骗的措施》，具体反诈措施涉及从个人到企业，从立法到普法的方方面面。爱尔兰加尔达国家网络犯罪局发布《网络犯罪风险和防治建议》，包含网络犯罪风险信息和网络犯罪预防措施，支持信息技术系统所有者和用户开发并实施适当的犯罪预防技术。中国公安部、国家发展和改革委员会、工信部、中国人民银行联合印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》，旨在打击治理涉诈黑灰产犯罪。在中泰缅老等联合打击专项行动中，除了打击电诈网赌犯罪本身之外，还打击网络诈骗、赌博衍生出的人口贩运、绑架、非法拘禁等刑事犯罪，打深打透电诈窝点，打残打断产业链条。

## 2. 优化跨国执法合作，国际法发展取得进展

网络犯罪的跨国性和复杂性的特征日趋凸显，依赖传统的国家治理机制难以抵御各类新型网络犯罪带来的风险和安全隐患，探索建立网络犯罪跨国合作治理模式是现实之需。2024 年，美国和澳大利亚签订《美国政府与澳大利亚政府为打击严重犯罪而获取电子数据协议》已经生效。该协议有助于美国和澳大利亚的执法机构及时访问电子数据，以预防、检测、调查和起诉严重犯罪。澜沧江－湄公河合作第九次外长会在泰国清迈举行，并发表《澜湄合作框架下加强打击跨境犯罪合作的联合声明》。声明强调，当前跨境网赌电诈、网络犯罪等跨境犯罪活动的严重性及其带来的威胁持续上升，危害澜湄地区安全稳定和人民安全幸福。各国重申将坚决打击跨境犯罪，确保公共安全、次区域稳定及人民生命和财产安全。

2024 年 12 月 27 日，联合国发布由 193 个成员国通过的《联合国打击网络犯罪以及为打击利用信息通信技术系统实施的某些犯罪并共享严重犯罪电子证据而加强国际合作公约》（以下简称《公约》）。《公约》是由中国、俄国等金砖国家倡导并引领推动，在广大发展中国家持续努力下促成的，也是互联网诞生以来，国际社会首次在全球范围内就网络犯罪打击达成的一项具有法律约束力的公约，对网络空间国际法发展有重要的指标性意义。

在《公约》正式出台之前，国际社会缺乏一个统一且具有约束力的法律框架来规范和打击网络犯罪，已经达成的一些多边条约，如《布达佩斯公约》《阿拉伯国家联盟打击信息技术犯罪公约》等，从适用范围和代表利益方面审视，均不具备“全球性”标准。《公约》将成为一个高效实用的法律工具，用于开展国际合作，预防和打击网络犯罪活动，并确保及时合法地收集、共享关于可能使用信息通信技术系

统实施的、涉及面广泛的电子证据。

《公约》首次把网络主权理念转化为具有约束力的规则，明确各国在履行义务时，要恪守主权平等、领土完整、不干涉内政等原则，强调在开展国际合作方面，充分保障和尊重缔约国司法主权，将对国际合作产生积极影响。

### 3. 豁免再度成为关注，安全研究人员保护纳入修法视野

“白帽子”是互联网中的俚语，指的是利用自身特殊技能，对目标信息系统进行检测扫描的漏洞发现者，因其出于维护信息系统安全的善意目的，不同于传统意义上利用漏洞进行恶意攻击或数据窃取等行为的黑客，故“白帽子”被认为是道德黑客或网络安全专家。多年以来，各国的网络安全人才、知识产权保护、网络安全防范和刑事立法涉及了“白帽子”等网络安全研究人员的法律地位、行为的违法性和边界等问题。2024 年“白帽子豁免”成为英国、德国等一些国家的刑事立法、修法关注点。英国政府正在重新审查《计算机滥用法》，因为目前的法律规定有可能将使用黑客技术作为其职责一部分的网络安全专业人员定罪，例如研究人员和渗透测试人员。修改后的《计算机滥用法》可能包括加强对道德黑客的保护和更新制裁制度，以应对日益复杂的网络威胁旨在遏制日益严重的网络犯罪问题。德国联邦司法部起草的新法案《刑法典-计算机刑法现代化》，旨在为负责发现并向供应商报告安全漏洞的安全研究人员提供法律保护。法案明确在合法范围内进行的网络安全研究活动将不再受到刑事追责，旨在确保白帽黑客和安全专家在保护公共安全的同时免于法律风险。

## 二、2025 年全球网络安全政策法律趋势展望

基于过往的持续跟踪，并特别结合对 2024 年以来的全球网络空间政策立法观察，可以预见，各国在网络安全方面的博弈与竞争、合作与协同将持续演进且更为复杂。这种复杂性不仅源于人工智能、量子计算等颠覆性技术的加速变革，还涉及地缘政治竞争与博弈、国家主权、安全和发展利益维护、国际秩序维护与重构等多重因素的妥协与碰撞。2025 年 1 月 20 日，美国总统特朗普正式宣誓就任美国第 47 任总统，其“独树一帜”的政策主张和外交策略，将为全球网络空间版图的未来发展注入诸多不确定性与新变量，促使各国在网络主权、数据跨境、出口管制、供应链安全、内容治理等领域的博弈态势更趋激烈，但国际社会也会在预演、适应、调整中将开辟新的方向和路径。2025 年 1 月，中国现象级人工智能 Deepseek 震撼全球，掀起新一轮技术革命与产业变革浪潮，为 AI 发展注入新的活力与动力，也将引发相关政策和法律调整。Deepseek 一经问世，便引起产业界、科技界以及各国政府、监管机构的高度关注，同时也遭遇了大量网络攻击和域外法律制裁。可以预见，AI 领域将迎来新的机遇和挑战，一个更加开放、创新、多元化和竞争的时代正在加速形成，国际社会的政治格局和法律环境无疑将更加错综复杂。

此外，全球南方国家的崛起与复兴，特别是新兴经济体在网络技术、数字经济方面的迅猛发展，正在逐步改变当下全球网络空间权力结构和制定规则，这些国家对网络主权、数字公平、隐私保护等议题深度关切，进一步推动全球网络空间政策法律更多考虑多元利益平衡，加剧治理复杂性。从中国乃至全球视角展望 2025 年乃至更长时期内，网络空间政策法律或将呈现以下趋势：

## （一）合作与竞争持续同频共振，企业出海法律环境更为复杂

国家间、区域间的竞争与合作仍会一如既往地持续并存，经济和科技领域的博弈可能进一步加深技术代差和全球割裂。拜登政府临卸任之际，频繁在 AI、芯片等尖端科技领域出台对中国的限制措施。而欧盟、加拿大、英国等以单一市场、环保能源、个人数据和国家安全等为由，频繁制造国际数字贸易的壁垒和障碍。《瓦森纳协定》、EAR 等旧有的规则仍在继续堆叠施压，新的更严厉的框架则可能正在串联和形成中。随着中美科技竞争加剧，新上任的特朗普政府大概率会延续拜登政府“小院高墙”政策。由于美国、欧盟、中国等大国关系直接牵动全球格局，中国、美国及欧盟等重要经济体将继续呈现竞争与合作并存的态势，另一方面，随着“全球南方”国家在世界舞台上的影响力日益显著，以及“早期”企业出海的风险传递，又必然推动着出海向更深、更远之处拓延，企业出海既有机遇又必然面临更多障碍和围栏。

2025 年是中国提出“一带一路”倡议第二个十年的开局之年，中国一方面可能继续通过对内规则优化、对外推动适配和加入 CPTPP 等重要多边、双边协定等方式开拓和提供更广阔的营商空间和贸易环境；另一方面，也会进一步强化产业数字化转型和产能升级，并通过与沿线国家合作，将合作理念上升为进出口监管政策法律和规则层面，通过传导跨境合规理念和规则，为贸易发展和企业出海提供逆风而上的合规驱动力量。对于企业而言，尽管境内和跨境的多重监管将成为一种普遍，但通过将合规需要视为是第一准则，借助和利用网络空间合规的高效赋能，在国际竞争中积极探索寻求破局之道，企业的经营能力亦将有更大提升。

## （二）关基安全融入新型风险，供应链安全成为治理关键

关基安全已经成为全球各国网络安全保护中的一项长期性重点任务。随着人工智能等新技术的引入，供应链、数据安全等风险的日益凸显，除安全评估、风险监测等传统风险防御手段稳步推进以外，关基安全保护工作也将呈现新的特点。

一是如何基于人工智能、量子计算等颠覆性技术当前发展及未来潜能，准确预判、提前布局关基安全防御能力，使关基安全保护工作能够平稳、从容地适应信息技术的发展变化将成为各国考虑的因素之一。美国国土安全部在《美国关键基础设施安全弹性战略指南和国家优先事项（2024—2025 年）》中表示将把人工智能纳入战略考量，指出人工智能作为变革性技术在关键基础设施保护中的潜力与挑战，警惕人工智能技术滥用对关键基础设施带来的风险；同时，强调量子计算对现有密码体系构成的安全风险，DHS 将与 NIST 合作制定指南文件，帮助关键基础设施实体应对量子计算带来的密码和数据安全挑战。国土安全部发布的《2023-2027 财年战略计划》中也将评估和应对不断发展的网络和新兴技术风险列为“保障网络空间和关键基础设施安全”的四项具体任务之一。因此从供应链的新风险识别上，传统的 ICT 供应链安全内容将不可避免的重塑，以应对颠覆性技术带来的“降维”攻击。

二是在传统运行安全的基础上，供应链安全将更多成为关基安全保护工作的切入点。面对复杂多变的国际形势，以及供应链逐渐成为个别国家博弈的手段，如何确保关基供应链安全，充分借助网络安全审查、网络安全专用产品和关键设备检测认证、国产化、网络产品和服务提供者管理等制度工具，同步提升关基运营者对自身供应链的安全管理能力、网络产品和服务提供者融入关基供应链中的安全保护水

平，识别开源、人工智能等供应链环节的新“盲点”，确保从关基核心业务的持续性视角审视和保持将供应链安全成为关注点。

## （三）数据利用规则补足完善，数据法治扩展至生态治理

数据要素流通共享利用将愈加常态化，数据产业、生态将持续构建、完善。在此背景下，数据安全政策立法将呈现以下趋势：

一是提高数据领域动态安全保障能力将成为数据安全规则补足、完善的重要方向。作为数字经济时代的重要资源，数据要素安全直接影响数据价值释放。数据为发展赋能将成为各国数据法治的强烈政策导向，数据流转安全问题随着数据要素开发利用将愈加突出。数据流通利用安全规则将是下一个阶段数据安全规则补足、完善的重要方向。国内，在高质量发展成为全面建设社会主义现代化国家首要任务的背景下，无论是规则制定还是执法监管，均不可脱离产业发展实际或发展水平、发展需求谈安全。这就要求要结合发展形势关注发展中的安全问题，提升监管重点、方式与安全形势的匹配性。例如高度关注数据要素流转、加工、分析、融合、汇聚关联等安全风险。

二是适应和服务于数据产业发展，数据法治将从“安全”治理扩展至“生态”治理。数据采集汇聚、计算存储、流通交易、开发利用、安全治理和数据基础设施建设等数据产业将进一步蓬勃发展。数据安全问题不再是单点问题，而是会上下游传导，向其他主体辐射影响。随之而来的数据安全治理不再是对数据本身的治理，而是对整个数据产业链、生态链的治理。国内，发展数据产业是深化数据要素市场化配置改革、构建以数据为关键要素的数字经济的重要举措。在此背景下，数据生态治理这一特点将在接下来数据要素发展中体现得尤为明显。

三是数据跨境传输规则将仍是数据安全法治的重要变量。全球主

要经济体对数据治理规则制定的主导权争夺进一步激化，数据治理模式竞争性特点进一步凸显。作为全球数据治理的重要议题，数据跨境流动受地缘政治影响程度也将进一步扩大。主要经济体在数据跨境流动方面的规制分歧在相当长一段时间内难以弥合，利益相关方在数据跨境流动方面的价值共同体建设将持续加强，数据跨境流动未来将面临仍将面临诸多复杂性与不确定性。从《网络安全法》到《数据安全法》《个人信息保护法》再到后续《数据出境安全评估办法》《促进和规范数据跨境流动规定》《网络数据安全管理条例》的出台，中国数据出境规则、机制逐渐发展、调整和完善，可以说当前数据跨境监管框架基本搭建完成，但数据跨境仍然存在诸多细化问题需要进一步研究和解决，包括重要数据的识别判定、自贸区负面清单制度探索尺度等等，这些都是面向各类数字贸易新协定时亟需解决的迫切问题。

四是数据基础制度探索依然是包括数据安全在内的数据法治的重要任务。长期以来，数据权益问题是影响数据供应及数据利用的重要因素。从全球范围来看，当前仍未有一个成熟的解决方案。加强顶层设计、总体谋划，抓好数据产权、流通交易、收益分配、安全治理等政策制定，加快构建适应数据要素特征、符合市场规律、契合发展需要的基础制度已成为完善数据要素市场制度规则的重要要求。近年中国在培育发展数据要素市场实践基础上探索出了数据资源持有权、数据加工使用权、数据产品经营权等分置机制，但仍存在诸多基础性问题有待解决，也直接影响数据安全治理。后续数据基础制度探索依然是包括数据安全在内的数据法治的重要任务，在既有的立法规制掣肘的情况下，通过典型司法案例和适当的弹性释法将可能成为有效地回应市场关切和展现示范效应的手段。

## （四）个人信息保护规则调整，回应人工智能技术发展需求

全球个人信息保护将延续制度规则不断细化、完善与调整的趋势，尤其是针对特殊类型、特殊场景、特殊主体个人信息保护的规则进一步明确。针对个人信息保护基础和重要制度落实的监管力度持续加大。同时，以人工智能为代表的新技术对个人信息与隐私保护规则的冲击进一步凸显。

一是个人信息保护制度深化落实，个人信息保护治理效能稳健提升。未来，各国监管机构持续推进个人信息保护制度落地，部分相对原则性的规范得到澄清，个人信息保护规则在具体场景、领域的适用标准得到进一步明确，探索个人信息治理效能的稳健提升是应有走向。就中国个人信息保护工作而言，作为评价相关主体个人信息处理活动遵守法律、行政法规情况的重要制度，且网安标委已经组织开展《数据安全技术 个人信息保护合规审计要求》试点工作，个人信息保护合规审计制度落地实施在即。而对于《网络数据安全管理条例》规定的个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等制度间如何实现衔接，是监管机构下一步需要重点回应的问题。企业方面，系统化推进个人信息保护制度要求融入业务活动，尤其是在技术层面探索安全模型以降低个人信息安全风险，将落实个人信息保护义务内化为个人信息安全保护能力是实现合规的必然趋势。

二是人工智能技术与个人信息、隐私保护规则之间的冲突或将获得回应。人工智能模型训练对自动化采集大量个人信息的需求与知情同意规则之间的冲突，以及处理目的非预设性、处理结果的难预知性也与个人信息保护的最小必要原则、目的限制原则、存储限制原则之间的冲突，愈来愈成为人工智能从“能用”迈向“好用”过程中无法回避的问题。中国《网络数据安全管理条例》规定使用自动化采集技

术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息的，应当进行删除或者进行匿名化处理，删除或者匿名化处理从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理，可以理解为对上述问题的初步回应。未来，随着人工智能迈入新的发展阶段，人工智能技术对个人信息保护规则的冲击进一步加强，将有更多国家及地区在立法层面关注这一问题，考虑如何避免过度关注个人信息保护形式要求，针对人工智能需求特点探索实质化保护方案，不排除美国、中国等对个人信息保护制度进行重构。

## （五）供应链安全治理在不同领域扩张，规则不确定性仍然突出

不仅局限于关基领域，供应链安全将仍可能是所有领域网络安全风险的重要来源，供应链安全规则的建设将仍是各国网络安全治理的重要内容。与此同时，在经济、政治等诸多因素影响下，供应链安全规则共识的达成任重道远，国际博弈、冲突将持续、深度影响供应链安全，供应链在关基领域的适用规制向非关基领域的扩张将成为趋势。

一是供应链安全治理在网络安全治理中的重要性将愈发凸显。在网络安全与供应链安全的紧密联系日益凸显的背景下，任何软件中的细微漏洞或供应链中的疏漏都可能被恶意利用，如何强化供应链安全将成为网络安全治理的重点关注。

二是地缘政治、国际竞争等将深度影响供应链安全规则。长期以来，供应链安全监管是美国对华竞争的重要工具。美国 2024 年 2 月发布的《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据行政令》以限制相关数据从美国向包括中国在内的受关注国家流入。其中一个重要原因就在于，美国政府认为受关注的国家可以依靠包括人工智能在内的先进技术来分析和操纵大量敏感的个人数据，以从事间谍活动、网络行动等或确定相对于美国的其他潜在战

略优势。2025 年 1 月，美国商务部工业和安全局发布的最终规则《保障信息和通信技术及服务供应链：网联汽车》禁止销售或进口集成了特定硬件和软件的互联汽车，或单独出售的组件等措施均是这一特点的体现。后续地缘政治、国际竞争等因素对影响供应链安全规则的影响将持续显现。

三是开源软件安全监管规则将成供应链安全规则完善重点。开源模式已成为全球软件技术和产业创新的主导模式，开源软件或组件是网络系统中庞大软件体系的主要基础。同时，开源软件漏洞危害大，波及范围广等问题也日益突出。xz 供应链安全事件就充分暴露出供应链脆弱性给网络安全带来的威胁。开源软件如何治理国际上尚未形成共识，国内也未建立明确规则。随着开源软件的日益普及应用，其安全监管规则将成供应链安全规则将成为下一阶段的完善重点。

### （六）信息内容治理政治性趋向加剧，关注人工智能非法应用打击

信息内容治理的政治性趋势历来显著，其深刻影响在诸如“茉莉花革命”、特朗普第一任期内对《通信规范法》的修订以及香港修例风波等事件中得到充分体现。这些事件不仅揭示了信息内容治理与政治环境的紧密联系，更凸显了大平台尤其是社交媒体在塑造社会舆论、影响政治进程中的关键作用。最近几年，欧盟、美国、中国等都重点夯实大平台尤其是社交媒体的信息内容治理责任，且不断强化执法。

随着算法和人工智能的深入应用，可以预见，全球范围内的网络信息内容治理将呈现出更为深入、精细和技术驱动的特点。一方面，各国将更加注重技术创新在治理过程中的核心作用，推动采用人工智能等新技术手段加强违法有害信息的识别监测，以更高效、精准地识

别、过滤和移除非法或有害信息。2024 年度立法中已经有所体现，例如中国的《网络暴力信息治理规定》明确“网络信息服务提供者应当采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络暴力信息的识别监测。”另一方面，随着生成式人工智能技术的不断成熟和广泛应用，其被用于生成、传播违法有害信息的风险也日益凸显。全球范围内的信息内容治理将更加注重预防和打击人工智能的非法应用，限制和禁止利用人工智能技术生成、传播违法有害信息将成为重要关注方面。

此外，从目前立法动向和政策导向来看，未来对大平台的认定会持续推进，欧盟层面将继续完善《数字市场法》《数字服务法》等相关法律法规的实施和监管机制；中国则会继续加强互联网平台的监管和认定工作。美国方面，随着特朗普第二任期的开启，信息内容治理的政治趋向性可能会更加明显。特朗普强调和倾向的“美国优先”政策理念会使得美国在处理网络安全空间相关问题包括信息内容治理时，更加注重维护美国政治和经济利益，不排除其利用信息内容治理推动政治议程。从 2025 年 1 月社交媒体巨头 Meta Platforms 取消事实核查计划的重大事件来看，未来的信息内容治理在美国将经历重大变革，欧盟、美国、中国关于信息内容治理的政策分歧也将更加明显。

## （七）人工智能法治综合发展，各环节协同演进

人工智能法治作为一个综合体，包括法律的制定和制度的运行，人工智能相关立法探索只是一个方面，还包括执法、司法和守法的法律适用。未来，中国 Deepseek 带来的深远影响将全面而深刻地渗透到技术革新、产业升级以及政策法律的多个维度，推动这些领域向更深层次、更广范围迈进。如果说 2024 年是各国逐步熟悉人工智能安全风险、筑法治之基、积法治之势的一年，那么接下来将是各国行法

治之力、推动人工智能监管治理纵深发展的一年。

一是针对大模型的执法重点有望从数据与隐私保护向透明度和可解释性、供应链安全等方面进一步拓展。以欧盟为例，多部法律将协同适用，执法呈现出明显的严格化、精细化和跨领域协作特点。2025年不仅是欧盟《人工智能法》实施元年，也将进入《通用数据保护条例》《数字服务法》《人工智能法》等多部重要法律并行实施的关键节点，跨领域执法的全面性将进一步凸显，开启欧盟对人工智能领域系统性监管的新时代。高额罚款和跨境集体诉讼将更为频繁，“操纵性、欺骗性和剥削性人工智能系统”等关键概念将在具体案件中得到深入分析和验证，直接影响法律执行效果和企业合规义务。在此背景下，跨国企业的合规任务将更为艰巨，需要在多个法律框架下重新审视和调整业务模式、数据处理流程和技术应用等方面，以确保全面符合欧盟法律要求。中国的网信、公安等部门针对生成式人工智能的执法重点将进一步清晰，生成式人工智能服务提供者未按规定开展训练数据处理活动、未明确并公开其服务的使用人群和场合、不履行内容管理义务等将成为执法关注点。

二是如何平衡发展与安全、创新与责任、公益与私益、成本与收益等多重目标与任务之间的内在张力，是未来人工智能法治的关键问题。在大国战略竞争回潮的背景下，美欧出口管制重点领域从半导体技术、先进芯片制造设备向云计算服务、数据获取方面蔓延。未来人工智能算法、算力和数据相关的国际规则制定权和制度领导权也将成为各国争夺的重要目标。

三是各国有望从针对生成式人工智能、深度合成等特定技术的监管趋向更加技术中立的包容性监管，抑或是探索设置动态清单使人工智能综合监管框架更具备可扩增性。面对不断创新、迭代的大模型技

术、应用和服务，监管需要的是动态性、发展性的视角，而不是依赖于静态、僵化的治理类别。技术进步以及对人工智能与社会之间互动的理解也将反映在各国人工智能监管实践中。

四是各国有望从针对生成式人工智能、深度合成等特定技术的监管趋向更加技术中立的包容性监管，抑或是探索设置动态清单使人工智能综合监管框架更具备可扩增性。面对不断创新、迭代的大模型技术、应用和服务，监管需要的是动态性、发展性的视角，而不是依赖于静态、僵化的治理类别。技术进步以及对人工智能与社会之间互动的理解也将反映在各国人工智能监管实践中。

五是人工智能研发与应用具有很强的全球性特征，需要各方从不同的认知理解和期望需求中寻求共识和互信，推动智能向善，增进人类共同福祉。各国将更为关注健全人工智能国际合作治理对接机制，把治理共识转化为具体行动、把理念认同转化为务实成果，联合国人工智能高级别咨询机构、金砖国家组织人工智能研究组等将有更多成果输出和实际影响。同时，未来人工智能算法、算力和数据相关的国际规则制定权和制度领导权也将成为各国争夺的重要目标。

## （八）密码法治持续完善，技术革新与政策响应同步加速

展望未来，密码法治必然加速调整落实，技术革新与政策响应同步加速，这根植于全球数字化转型带来的国内外竞争与安全秩序需求变化，也体现了密码技术革新对政策法律制定的驱动作用。

一是国际网络安全形势的不稳定性、不确定性更加突出，各国密码攻防博弈复杂激烈。全球正步入量子时代的前夜，技术革新与政策响应正同步加速。量子计算、后量子密码等颠覆性、前沿性技术竞争优势的争夺不仅会继续体现在相关政策立法、投资、标准化和国际合作层面，更会实质性进入不同产品、技术、服务形态的出口管制和执

法个案层面。

二是 PQC 标准化进程持续推进，且将在密码实际部署和应用中占据核心地位。2024 年 NIST 发布三项 PQC 标准，引起业界广泛关注和深远影响，为后续更多 PQC 算法跻身标准之列奠定基础。未来，欧盟、中国、国际标准化组织等也将积极投身其中，征集、制定先进 PQC 标准或指南，PQC 重点将同步转向实际环境中的部署与应用，政府部门、关基、关键行业、重要系统和数据等对安全性要求较高的领域，将依据既定的优先级顺序，分阶段、有步骤地推进迁移工作。

三是中国《密码法》《商用密码管理条例》进一步贯彻贯彻落实。智慧中国和数字社会建设步伐加快，给密码应用和随之而来的密码管理工作带来前所未有的机遇，各地密码管理部门的监督检查、行政执法工作将进一步深化。

四是中国密码服务大局价值进一步凸显。新时代创新发展、服务大局要求密码工作必须围绕国家创新驱动发展战略，推动密码科技自主创新和跨越式发展的同时，服务好高水平对外开放。包括不限于在中国密码企业高水平“走出去”、“一带一路”共建、数据要素制度体系构建等战略中充分发挥密码科技以及密码法治功能，大力推动商用密码应用促进和贸易繁荣。发挥《密码法》作用，在 WTO 多边贸易体制、区域贸易协定和中国自由贸易港法规等中积极塑造以我为主的密码政策，为密码相关的应用促进和贸易提供制度保障，将成为密码法治重点发展方向。

五是技术和产业发展进一步驱动中国政策法律制定。中国后量子密码正在进入第一个发展繁荣期，国内有关行业和企业都在积极探索后量子密码的应用和布局，国内抗量子法律政策出台整体滞后于技术和产业发展。可以预见的是，后量子密码算法战略和政策法律研究、

《密码法》的后量子密码法律适用和创新发展问题研究，如何实施国家技术动员并确立我国后量子解决方案的路线，如何构建国际后量子密码算法、产品和服务发展监测体系，如何培育中国后量子密码创新生态机制，必然成为 2025 年乃至更长时间内中国政策法律领域的重大问题。

## （九）虚拟货币发展迅猛，完善安全监管成为必然

近年来虚拟货币的资产属性更加凸显，已经成为全球数字经济及科创发展的必争之地。2025 年 1 月，特朗普在上任的第一周即签署相关行政令，将支持数字资产、区块链技术以及相关技术在经济各个领域的负责任增长和应用。特朗普政府期望通过稳定币立法，确保美元在国际上的主导地位，增加美元的数字使用。美国证券交易委员会成立“加密货币工作组”，旨在为加密资产制定全面、清晰的监管框架。中国召开了中央政法工作会议，会议明确提出“针对虚拟货币等新问题，司法部要主动研究提出立法建议”。在此背景下，2025 年将开启加密货币 2.0 时代，美国无疑将为加密货币行业构筑更为友善的政策环境，其他国家的立法也将加速制定或者调整。

一是虚拟货币具备一般等价物属性、去中心性和匿名性，在当下和未来一段时期内将构成制裁和反制裁的重要手段。未来各国立法可能结合虚拟货币发展态势，探寻更多适合自身的反制裁措施。

二是随着比特币、泰达币等逐渐被认可为价值存储手段，部分国家、地区可能考虑将虚拟货币纳入国家储备，实现资产的多元化配置，尤其是美国总统特朗普对虚拟货币的支持，将对国际货币体系产生深远影响。美国、巴西、日本、德国、迪拜、中国香港地区已经或正在研究将比特币作为战略储备相关议题。可以预见，在特朗普新任期及更长时间，加密货币等将引来更加激烈的关注和竞争。

三是合法“挖矿”行为将进一步进入立法和执法视野，延续2024年特点，为保护能源环境，将有更多国家和地区关注合法“挖矿”的流程，打击虚拟货币挖掘过程中的违法能源消耗活动。

四是打击涉虚拟货币犯罪活动也将成为各国相关政策法律的关注重点。主要国家和地区如何在实践中加强金融科技手段对加密货币的监管应用，运用人工智能、区块链、云计算等开展涉虚拟货币可疑交易分析，探索建立监管沙盒等，值得关注。此外，完善涉案虚拟货币处置路径和制度是重中之重。虚拟货币的匿名性、去中心化、易跨境性等特征给司法部门的处置能力和传统涉案财物处置规则带来挑战，各国立法和实践探索将向此方面倾斜。

## （十）科学化与法治化交融，趋向生态治理和干预治理转型

在跨国网络犯罪的打击治理中，犯罪预防和打击惩治将进一步融合，由被动的刑事打击到主动的风险预防、由后端的犯罪结果规制到前端的源头治理。各国执法机关已然意识到，跨国网络犯罪治理不能单纯依赖刑罚和打击措施，应深刻认识犯罪生成的规律特点，充分考虑不同因素在犯罪生成中的地位和作用，进而采取科学、精准的防治对策。出于社会投入与收益的考量，各国近来已关注到结合犯罪预防的节点将刑事司法资源融入事前、事中和事后阶段，即刑事立法、刑事司法和犯罪矫正等程序。

中国正在加快制定《网络犯罪防治法》，探索构建网络犯罪生态治理制度，对黑灰产业链条中类型化的行为予以法律规制。同时，中国作为联合国打击网络犯罪公约的推动者和引领者，下一步将推动国内法与国际法衔接。目前各方同意在谈判成功约两年后启动一个专门解决定罪问题的附加议定书谈判，为扩大定罪保留窗口。中国如何在跨境网络犯罪治理生态塑造中从区域治理向国际治理，推动和率先批

约的国家利用好公约各项机制，积极就预防和打击网络犯罪开展合作，培育多层次、有弹性的犯罪治理生态，是一个需要考量的现实问题。

整体而言，全球网络犯罪治理正在逐步摆脱以刑事治理为主线、以刑罚威慑为手段的传统路径依赖，有望逐步迈入预防优先、强化生态治理和干预的治理图景和阶段之中。

# 附件：全球网络安全政策法律领域 2024 年大事件

## 一、境外网络安全政策法律领域 2024 年十大事件

### （一）联合国发布首个打击网络犯罪公约，具有全球性法律约束力

12 月 27 日，联合国发布 193 个成员国通过的《联合国打击网络犯罪以及为打击利用信息通信技术系统实施的某些犯罪并共享严重犯罪电子证据而加强国际合作的公约》，主要内容包括：（1）明确刑事犯罪。确定的刑事罪名包括非法访问、非法拦截、干扰信息通信技术系统等；（2）确立程序措施和执法手段。要求缔约国采取必要的立法和其他措施，开展快速保全电子数据、快速保全和部分披露流量数据等，以便进行具体的刑事侦查或诉讼；（3）促进国际合作。合作目的包括刑事犯罪侦查、起诉和与之相关的司法程序等。

### （二）欧盟《网络安全条例》正式生效

1 月 7 日，《欧洲议会和理事会 2023 年 12 月 13 日关于欧盟机构、团体、办公室和代理机构采取高水平网络安全共同措施的第 2023/2841 号条例》（《网络安全条例》）生效，旨在确保欧盟各机构、团体、办公室和代理机构采取共同的网络安全规则和措施，提高欧盟机构内部网络安全恢复和事件响应能力。《条例》将“欧盟机构、团体和代理机构计算机应急响应小组”更名为“欧盟机构、团体、办公室和代理机构网络安全服务”，但仍保留“CERT-EU”的简称；设立机构间网络安全委员会，以推动并监测本条例的实施。此外，《条例》建立了网络安全风险管理、治理和控制框架。

## （三）欧盟《人工智能法》正式生效

8 月 1 日，欧盟《人工智能法》正式生效，旨在促进欧盟单一市场中公共和私营行为者开发和采用安全和值得信赖的人工智能系统；同时确保尊重欧盟公民的基本权利，刺激欧洲对人工智能的投资和创新。这是世界上首部人工智能综合性立法，试图为人工智能监管设定全球标准。《人工智能法》遵循“基于风险”的方法，对社会造成危害的风险越高，相应的监管规则就越严格。该法仅适用于欧盟法律范围内的领域，并为部分系统规定了豁免，例如专门用于军事和国防目的以及研究目的的系统。

## （四）欧盟委员会通过 NIS2 指令首个实施条例

10 月 17 日，欧盟委员会根据 NIS 2 指令通过首个实施条例，对 11 类实体的供应链安全、网络安全、漏洞处理等网络安全风险管理措施提出具体要求，其中要求制定、实施和应用供应链安全政策，明确供应商和服务提供商选择标准，使得 NIS 2 指令可以真正落地实施。同时，条例明确重大事件判定的通用标准，包括造成的经济损失、是否涉及商业秘密泄露、是否导致自然人死亡或对健康造成重大损害、是否造成严重中断等，并针对 11 类实体提出特殊判定标准。

## （五）欧盟《网络弹性法》正式生效，提高数字产品安全

12 月 10 日，欧盟《网络弹性法》（CRA）正式生效，这是欧盟首部对包含数字元素产品的强制性网络安全法律文件，全面规定数字产品的网络安全要求、制造商和相关市场主体的责任义务，同时强化监管执行机制，覆盖数字产品全生命周期。CRA 适用于具有数字元素的产品，且其预期用途或合理可预见的使用范围涉及与设备或网络的直接或间接连接。CRA 对各类经济运营者的网络安全责任进行规

定，制造商是核心责任主体，要求其应当在产品设计、开发和生产阶段始终考虑并融入网络安全基本要求。

## （六）美国白宫发布《关于防止受关注国家访问美国公民大量敏感个人数据和美国政府数据的行政令》，司法部发布最终规则

2 月 28 日，美国白宫发布《关于防止受关注国家访问美国公民大量敏感个人数据和美国政府数据的行政令》，指示美国司法部制定保护敏感个人数据和政府数据不被受关注国家获取和利用的禁止性、限制性新规。同日，美国司法部发布落实行政令指示的拟议规则制定预通知。12 月 27 日，司法部发布《防止受关注国家或涵盖人员访问美国敏感个人数据和政府数据的规定》的最终规则，明确受管辖的数据类型及数据量门槛、受关注国家、禁止和限制的交易类型、豁免交易、合规机制等内容。

## （七）美国白宫发布《关于关键基础设施安全和韧性的国家安全备忘录》

4 月 30 日，美国白宫发布《关于关键基础设施安全和韧性的国家安全备忘录》。备忘录明确美国提升关键基础设施安全和韧性的目标，包括：（1）厘清各联邦机构在关键基础设施安全、韧性、风险管理方面的角色和责任；（2）基于风险识别和优先排序，对关键基础设施的安全和韧性进行分析，并实施协调一致的方法评估、管理安全风险；（3）建立关键基础设施安全和韧性的最低要求和问责机制，通过一致且有效的监管框架；（4）利用联邦政府协议，包括赠款、贷款和采购程序，要求或鼓励关键基础设施所有者和运营者达到或超过最低安全和韧性要求；（5）增强和改善关键基础设施威胁的情报收集和分析质量；（6）通过与国际合作伙伴和盟友合作，加强对关

键基础设施安全和韧性的态势感知，在全球范围内促进有效的关键基础设施风险管理合作，制定并推广关基安全和韧性的国际建议。

## （八）美国通过《TikTok 剥离法》，TikTok 要求认定该法违宪遭遇败诉

4 月 24 日，时任美国总统拜登签署一揽子立法，包含经过修订的《TikTok 剥离法》，对 TikTok 的母公司字节跳动剥离控制权时限规定为 270 日内，即 2025 年 1 月 19 日内，并授权美国总统可以将该时限最多再延长 90 日。若字节跳动未能在规定时限内将 TikTok 美国业务出售或以其他方式剥离，将面临全美禁令。

5 月 7 日，TikTok 向美国联邦法院提起诉讼，要求法院裁定《TikTok 剥离法》中限制 TikTok 的条款违宪。7 月 26 日，美国司法部首次对 TikTok 提起的联邦诉讼作出回应，称 TikTok 收集了 1.7 亿美国用户的大量敏感个人信息，可能通过收集数据及操纵算法影响用户所看到内容，从而威胁美国的国家安全和利益。12 月 6 日，美国哥伦比亚特区巡回上诉法院就此案作出裁决，认为该法不违反美国宪法。12 月 9 日，TikTok 向巡回法院申请紧急禁制令，希望阻止该法在 2025 年 1 月 19 日生效，以待最高法院复审。12 月 13 日，巡回法院驳回 TikTok 申请。12 月 16 日，TikTok 向美国最高法院申请临时禁制令，同时申请复审调卷令。最高法院在 2025 年 1 月 10 日进行复审，并于 1 月 17 日作出正式判决，以 9:0 裁定该法合乎美国宪法，要求其母公司字节跳动在 2025 年 1 月 19 日前剥离其在美国的业务，否则将面临全面禁用。

2025 年 1 月 20 日，美国第 47 任总统特朗普就任，并于当日签署行政令，要求《TikTok 剥离法》在未来 75 天内暂不执行。

## （九）美国 NIST 发布三份后量子密码标准

8 月 13 日，NIST 正式宣布推出首批三份后量子密码标准，旨在抵御量子计算机带来的网络安全风险。三项标准分别为:（1）FIPS 203: ML-KEM（Module-Lattice-Based Key-Encapsulation Mechanism），用于密钥封装，作为通用加密的主要标准；（2）FIPS 204：ML-DSA（Module-Lattice-Based Digital Signature Algorithm），作为保护数字签名的主要标准。该项标准基于 Dilithium 算法，专为数字签名设计;（3）FIPS 205：SLH-DSA（Stateless Hash-Based Digital Signature Algorithm），基于与 ML-DSA 不同的数学方法，旨在作为 ML-DSA 受攻击时的备用方法。

## （十）英国国王签署《2024 年调查权力法（修正案）》

4 月 25 日，英国国王签署《2024 年调查权力法（修正案）》，旨在扩张英国执法部门、情报部门（军情五处、秘密情报局和政府通信总部）和其他公共当局获取通信内容和通信数据的法定权力。修正案授权英国情报部门处理大量隐私程度较低的公民数据。情报部门负责人或相关执行任务的个人可以在获得司法专员授权且必要情况下，处理隐私程度低或不涉及公民隐私的数据。若遇紧急情况，上述主体可在未获授权情况下先行采取行动。此外，授权英国相关部门在特定情形下获取网络访问记录。在涉及国家安全、与国家安全相关的经济福祉、预防或打击严重犯罪时，英国安全部门、秘密情报部门、政府通信总部等有权获取特定个人、设备在特定时间内的网络访问记录。

## 二、境内网络安全政策法律领域2024年十大事件

### （一）党的二十届三中全会《决定》要求加强网络空间法治建设

7月15日至18日，中国共产党第二十届中央委员会第三次全体会议在京举行。全会审议通过《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》，提出健全网络综合治理体系。深化网络管理体制改革，整合网络内容建设和管理职能，推进新闻宣传和网络舆论一体化管理。完善生成式人工智能发展和管理机制。加强网络空间法治建设，健全网络生态治理长效机制，健全未成年人网络保护工作体系。《决定》要求完善公共安全治理机制。加强网络安全体制建设，建立人工智能安全监管制度。

### （二）中国提出《全球数据跨境流动合作倡议》

11月，习近平主席在亚太经合组织第三十一次领导人非正式会议上提出《全球数据跨境流动合作倡议》，并在2024年世界互联网大会乌镇峰会正式发布倡议全文。倡议就各方普遍关切的数据跨境流动治理问题提出建设性解决思路，明确中国促进全球数据跨境流动合作的立场主张，倡导秉持开放、包容、安全、合作、非歧视的原则，推动构建开放共赢的数据跨境流动国际合作格局，促进数据跨境高效便利安全流动。

### （三）《网络数据安全管理条例》正式公布

9月24日，国务院总理李强签署国务院令，公布《网络数据安全管理条例》，自2025年1月1日起施行。《条例》旨在细化、补充、完善《网络安全法》《数据安全法》《个人信息保护法》等法律规定的相关制度。条例提出网络数据安全管理总体要求和一般规定，

细化个人信息保护规定，完善重要数据安全制度，优化网络数据跨境安全管理规定，明确网络平台服务提供者义务。

### （四）《两用物项出口管制条例》正式公布

9 月 30 日，国务院总理李强签署国务院令，公布《两用物项出口管制条例》，自 2024 年 12 月 1 日起施行，主要包括管制政策、管制措施、监督检查等内容。《条例》保持现行两用物项出口管制体制稳定，明确国家出口管制工作协调机制、国务院商务主管部门、海关及其他有关部门的职责，取消出口经营者登记制度。此外，规定增强出口管制政策的透明度和规范性，明确政策制定的考量因素和程序，并且细化出口管制许可的便利措施及其适用条件和程序等。

### （五）国务院审议通过《公共安全视频图像信息系统管理条例（草案）》

12 月 16 日，国务院审议通过《公共安全视频图像信息系统管理条例（草案）》，指出要规范公共安全视频系统建设和使用，更好维护公共安全、保护个人隐私，是这一领域对社会和监管关注的重大回应。目前，草案正文尚未公布，4 月发布的征求意见稿对监控设备的设置位置、特定区域的监控使用以及紧急情况下的使用作出规定。职责分工方面，明确国务院公安部门负责全国公共视频系统建设、使用的监督管理和指导工作；县级以上地方人民政府公安机关负责本行政区域内公共视频系统建设、使用的监督管理和指导工作；县级以上人民政府有关部门在各自职责范围内负责公共视频系统建设、使用的相关管理工作。

## （六）中共中央办公厅、国务院办公厅印发《关于加快公共数据资源开发利用的意见》

9 月 21 日，中共中央办公厅、国务院办公厅印发《关于加快公共数据资源开发利用的意见》，围绕“深化数据要素配置改革，扩大公共数据资源供给”“加强资源管理，规范公共数据授权运营”“统筹发展和安全，营造开发利用良好环境”等五方面提出十七条意见。关于加强安全管理，意见要求强化数据安全和个人信息保护，加强对数据资源生产、加工使用、产品经营等开发利用全过程的监督和管理。建立健全分类分级、风险评估、监测预警、应急处置等工作体系，开展公共数据利用的安全风险评估和应用业务规范性审查。

## （七）四部门发布《互联网政务应用安全管理规定》

5 月 15 日，中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部联合发布《互联网政务应用安全管理规定》，规范各级党政机关和事业单位建设运行的互联网政务应用。网络和数据安全方面，要求建设互联网政务应用应当落实网络安全等级保护制度和国家密码应用管理要求，按照有关标准规范开展定级备案、等级测评工作，落实安全建设整改加固措施，防范网络和数据安全风险。中央和国家机关、地市级以上地方党政机关门户网站，以及承载重要业务应用的机关事业单位网站、互联网电子邮件系统等，应当符合网络安全等级保护第三级安全保护要求。

## （八）四部门印发《网络暴力信息治理规定》

6 月 12 日，国家互联网信息办公室、公安部、文化和旅游部、国家广播电视总局印发《网络暴力信息治理规定》，涉及预防预警、信息和账号处置以及保护机制等内容。《规定》要求，网络信息服务

提供者应当建立健全网络暴力信息预警模型，综合事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等因素，及时发现预警网络暴力信息风险。网络信息服务提供者发现涉网络暴力违法信息的，或者在其服务的醒目位置、易引起用户关注的重点环节发现涉网络暴力不良信息的，应当立即停止传输，采取删除、屏蔽、断开链接等处置措施，保存有关记录，向有关部门报告。

## （九）四部门印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》

11 月 27 日，公安部、国家发展和改革委员会、工信部、中国人民银行联合印发《电信网络诈骗及其关联违法犯罪联合惩戒办法》，自 2024 年 12 月 1 日起施行。《办法》主要包括惩戒原则、惩戒对象、惩戒措施、分级惩戒、惩戒程序、申诉核查等六方面内容，明确惩戒措施包括金融惩戒、电信网络惩戒、信用惩戒。

## （十）国家网信办公布《促进和规范数据跨境流动规定》

3 月 22 日，国家网信办公布《促进和规范数据跨境流动规定》。《规定》主要内容包括：一是明确重要数据出境安全评估申报标准；二是明确免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件；三是设立自由贸易试验区负面清单制度；四是调整应当申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件；五是延长数据出境安全评估结果有效期，增加数据处理者可以申请延长评估结果有效期的规定。